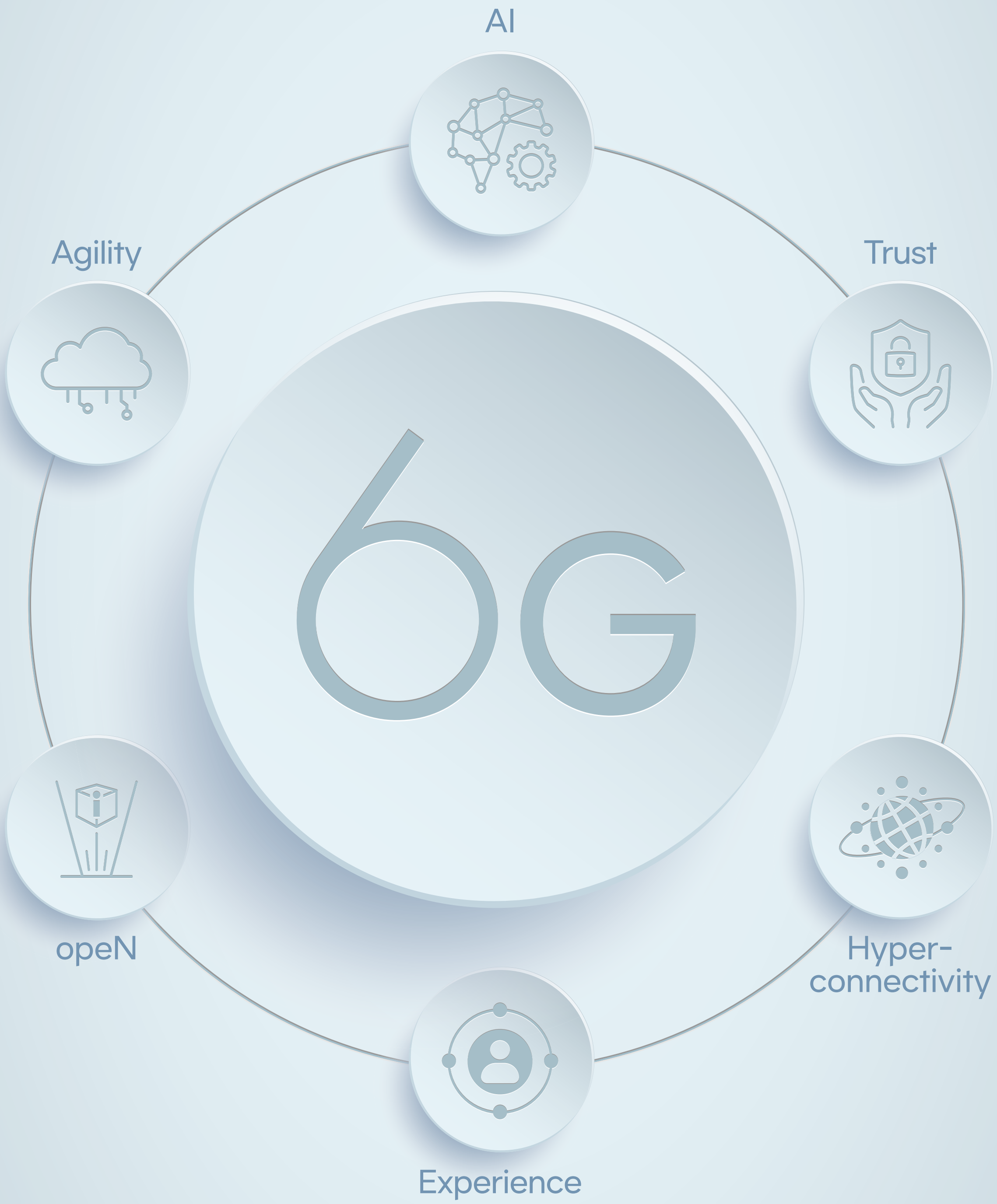
2026

SK Telecom 6G White Paper

Vision on Future Network Architecture, ATHENA



ATHENA

AI, Trust, Hyper-connectivity, Experience, opeN, Agility

Vision on Future Network Architecture

SK Telecom

Contents

Executive Summary

Introduction

- As the industry faces evolving dynamics including AI integration, service expansion, enhanced security requirements, and operational paradigm shifts, SK Telecom is charting its mid- to long-term network evolution strategy to drive operational efficiency, elevate customer experience, and unlock network monetization opportunities.

Mid- to Long-term Telco Infra Evolution Direction

- SK Telecom presents six network visions: ▶ AI-native ▶ Cloud-native ▶ Ubiquitous ▶ Open ▶ Zero-Trust ▶ Customer-centric.
- Mid- to long-term networks need to be designed to develop and apply domain-specific technologies, based on supporting new services for customer-centric value creation and efficient end-to-end operations.

Domain-Specific Technologies & SK Telecom's R&D Initiatives

- (Radio Access Network) Leveraging virtualization and open interfaces, the network will evolve toward AI-native RAN that autonomously performs intent-based optimization and AI service support, while aiming to implement continuous verification and protection of all access and data based on zero trust architecture. SK Telecom is strengthening its technological leadership as a mobile network operator and expanding the ecosystem through R&D in AI-driven performance optimization, RIC/orchestrator-based intelligence, and standards-based open interfaces.
- (Core Network) Future core networks will evolve toward autonomous operations in CNF and MSA-based cloud environments, leveraging AI for resource optimization, automatic recovery, and intent-based control. SK Telecom is driving this evolution by developing AI-based core automation and intelligent control technologies on centralized AI data centers,

maximizing operational efficiency through cloud-native transformation and agentic AI, and pioneering advances in API openness and security.

❍ (Transport Network) Evolution toward AI-native Converged TN pursuing intelligence and automation through AI-based integrated control and management and network digital twin environments is expected. To achieve this, SK Telecom is pursuing technology development to strengthen scalability, cost-efficiency, and security by developing APN architecture evolution, quantum cryptographic communication-integrated security, next-generation fronthaul technology, and Cross-DC xPU clustering.

❍ (DIVE) As a platform providing differentiated services and value based on network data, evolution toward hybrid edge-cloud architecture providing AI-based network data service and operation environments, dual plane deployment separating policy and service deployment, and ZTA is expected. SK Telecom is prioritizing development of hybrid edge-cloud architecture and AI-powered data service development technologies for precise indoor positioning location-based services, with plans to expand development scope in network data services.

Conclusion

❍ SK Telecom is preparing mid- to long-term networks on four pillars (AI, cloud, security, and open networks) to innovate operational efficiency and customer experience through intelligence and automation of radio access networks, core networks, transport networks, and data platforms.

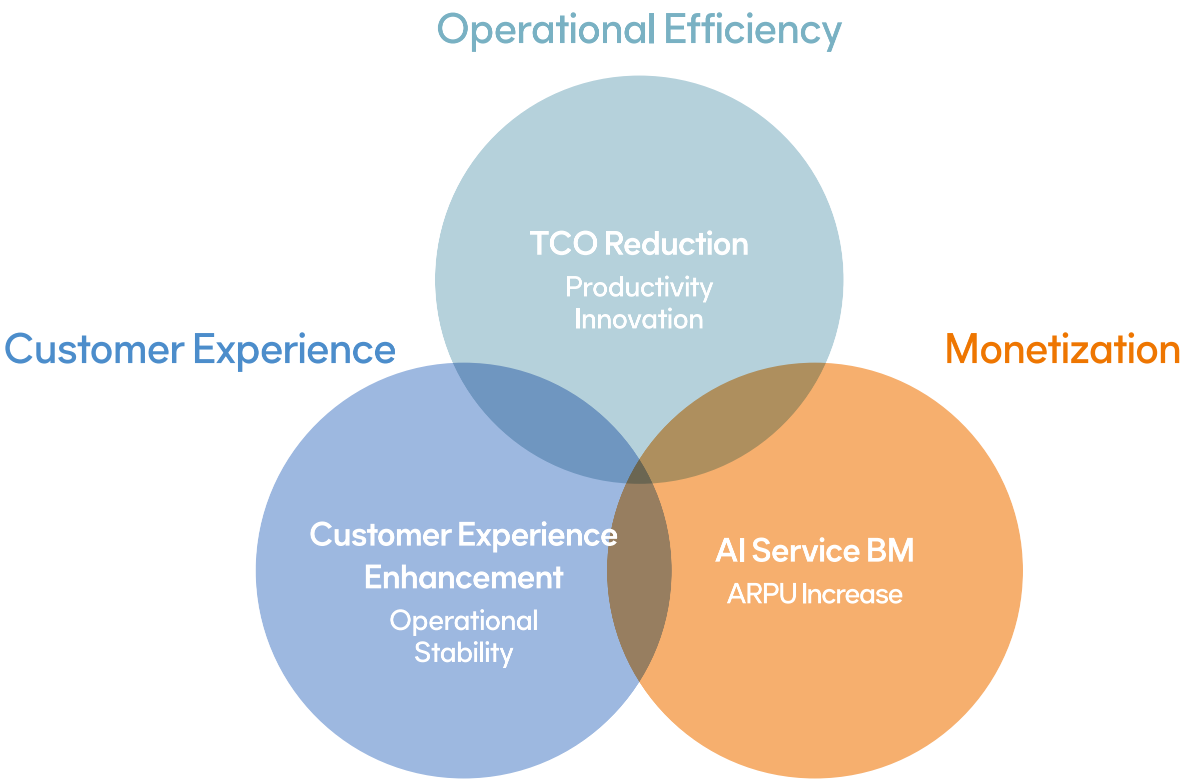
❍ Navigating 6G uncertainties with customer value at the center, SK Telecom is creating pioneering telecommunications infrastructure through AI-native and cloud-native transformation, fortified by open interfaces and zero trust security, to unlock new market opportunities.

* This document is provided for informational purposes only and does not constitute a promise or guarantee of any actual service or technology provision. The forecast information contained herein is subject to change depending on future standardization and technology development status.

1. Introduction

Six years after the world's first commercialization of 5G, the mobile communications industry is already looking ahead to 2030 and beyond, accelerating preparations for 6G, the next generation of mobile communication. Since 2023, SK Telecom has published 6G white papers every year, presenting the requirements and key technologies needed to prepare for the 6G era from a mobile network operator's perspective. The 2023 white paper proposed the key requirements of 6G derived from the experience of 5G commercialization and the direction of 6G technology evolution. Subsequently, the 2024 white paper presented a specific blueprint for 6G readiness by outlining the evolution of 'AI Telco Infra', which will lead to network intelligence [1][2].

This 2026 white paper proposes how the future network architecture should evolve from a more mid- to long-term perspective. The environment a decade from now, when 6G fully arrives, is expected to experience four major changes. The first is the convergence of AI technology and networks represented by 'AI Everywhere'. This holds significant meaning along two axes: AI for Network to enhance network performance, and Network for AI to support AI proliferation, both of which are expected to expand further. Second is the full-scale expansion of related services, including 5G-era innovations such as autonomous vehicles and multimodal AR/VR, as well as new services like Physical AI represented by



[Figure 1] SK Telecom's Direction for Network Architecture Evolution humanoids. These are expected to be commercialized on a large scale in the 6G era, requiring network architectures capable of supporting them. Third, concurrent evolution is expected in system architecture changes driven by service diversification, network virtualization and openness, and the advancement of security technologies to strengthen personal information protection. Finally, the transformation of network operation paradigms in response to rapid demographic and social environmental changes will also be an important consideration.

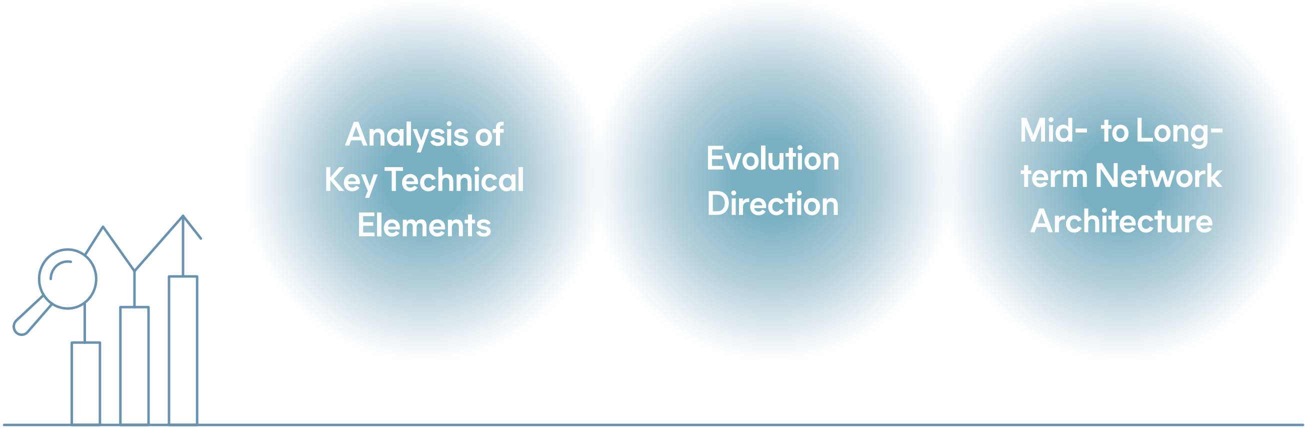
In the midst of these changes, as illustrated in [Figure 1], SK Telecom has defined three goals: 'Operational Efficiency', 'Customer Experience', and 'Monetization' with the goal of improving network operations in the mid- to long term. SK Telecom is also developing key technologies to achieve these goals by setting detailed quantitative KPIs for each goal.

Achieving mid- to long-term network goals requires comprehensive consideration of various factors beyond technical aspects, including future services and customer/market changes, investment and costs, and domestic and international policies. Particularly in the technical domain, discussions are needed across multiple dimensions such as spectrum, transmission technologies, and network architecture.

This white paper focuses on the components of mobile communication network systems, examines the evolution direction of each major area such as radio access network, core network, transport network, and network data platform, and introduces related technology trends and SK Telecom's research status.

2. SK Telecom's Mid-to Long-term Telco Infra Evolution

This section first presents the evolution direction of networks from a mid- to long-term perspective based on enabling technologies that directly affect the composition of telecommunication infrastructure. In addition, the telco infra architecture will be derived based on the proposed evolutionary direction, and its key components and roles will be explained in detail.



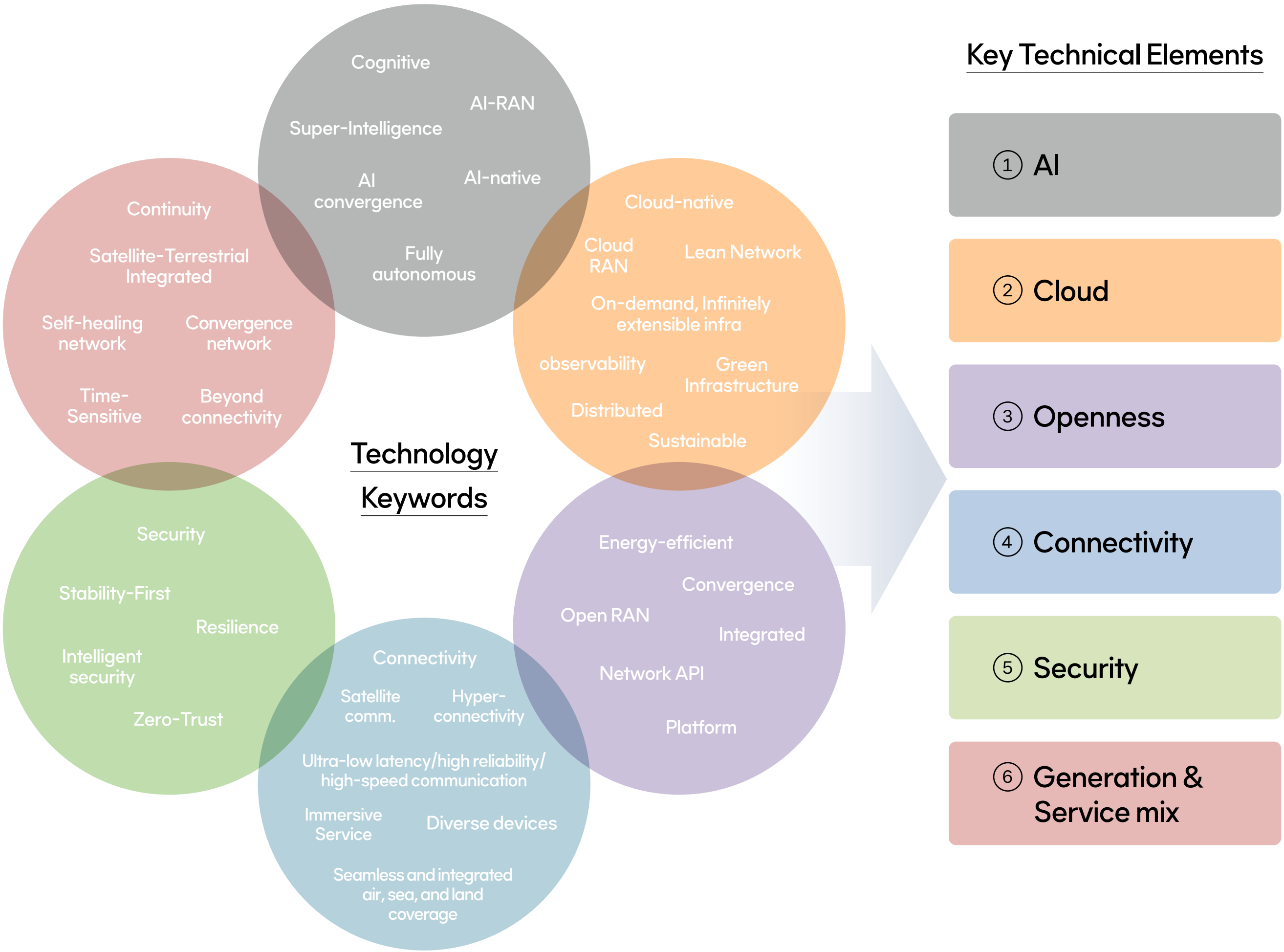
Analysis of Key Technical Elements

Evolution Direction

Mid- to Long-term Network Architecture

2.1 Analysis of Key Technical Elements

SK Telecom and major global mobile operators and vendors have each announced the key elements that 6G and mid- to long-term networks should have[3][4][5]. [Figure 2] examines enabling technologies for network composition, focusing on major technology keywords commonly mentioned among them.



[Figure 2] Key Technical Elements of Future Networks

① AI

The convergence of AI technology and networks is considered the most important factor in next-generation network evolution. In fact, research is actively underway to improve network processing and operation performance by applying AI to the communication domain, and at the same time, discussions are also being held on the role of networks to support AI services more efficiently. In addition, AI technology is being actively used to advance the performance of AI models by utilizing the vast amount of data generated by the network, while also innovating services from the customer's perspective, such as spam blocking.

② Cloud

Virtualization technology, which evolved in data centers, has expanded to the field of mobile communication and continues to develop. In the early days, VM (Virtual Machine)-based NFV (Network Functions Virtualization) was the mainstay, but recent evolution toward lightweight and scalable container-based approaches has accelerated mobile network adoption. Containers have less resource overhead than VMs and can be quickly deployed and scaled in microservice units, making them more suitable for large-scale mobile network operations.

In the field of radio access networks, the adoption of vRAN (virtualized RAN) technology is also active, and existing equipment vendors and IT companies have launched commercial solutions, and some North American, European, and Japanese operators have commercialized them in specific regions.

③ Openness

Open technology development is progressing to enable flexible network operation and cost efficiency. The importance of expanding the application scope and standardization of "Open Interfaces" for interworking between different manufacturers is growing. Notably, in radio access networks, the ecosystem around O-RAN Alliance-led Open Interfaces is becoming active. The GSMA's CAMARA project is conducting activities to open network assets owned by mobile network operators—such as QoS, location information, security, and authentication—to third parties through standardized APIs.

Beyond interface openness, movements to improve open network architecture are rapidly spreading, including the introduction of COTS (Commercial Off-The-Shelf) hardware, application of cloud-based virtualization solutions, utilization of open source, and Open RAN architecture design.

However, except for cases where open interfaces have been introduced in some equipment, most manufacturers are still developing commercial products based on their own interfaces and configuration parameters, making interworking between heterogeneous manufacturers difficult. Therefore, technology development to address this challenge is necessary.

④ Connectivity

As mobile communication generations evolve, technology development to strengthen connectivity continues to hold significant importance. Technical discussions are underway to improve radio access network coverage and performance through E-mMIMO (Extreme massive Multiple Input Multiple Output) and AI/ML-based RAN optimization. Convergence technology development between terrestrial networks and NTN (Non-Terrestrial Network)—including satellites and aerial networks—is also progressing.

In transport networks, following the advancement of optical transmission technology, technology development to simplify network architecture and simultaneously realize high-capacity, high-speed data transmission and scalability is accelerating. This is achieved by converging previously separated IP networks and backbone networks through IPoDWDM (IP over DWDM), transmitting IP packets directly at the optical layer.

⑤ Security

As IT, OT, and CT converge into a complex ecosystem, security by layer and by service based on ZTA (Zero Trust Architecture) is being emphasized, moving beyond traditional transmission layer-centric security. For example, the 5G specification has considered structural security improvements such as the introduction of SUCI (Subscription Concealed Identifier). Continuous mutual authentication and traffic encryption are essential. Security is being strengthened from the perspective of the entire communication system, including the initial access procedure.

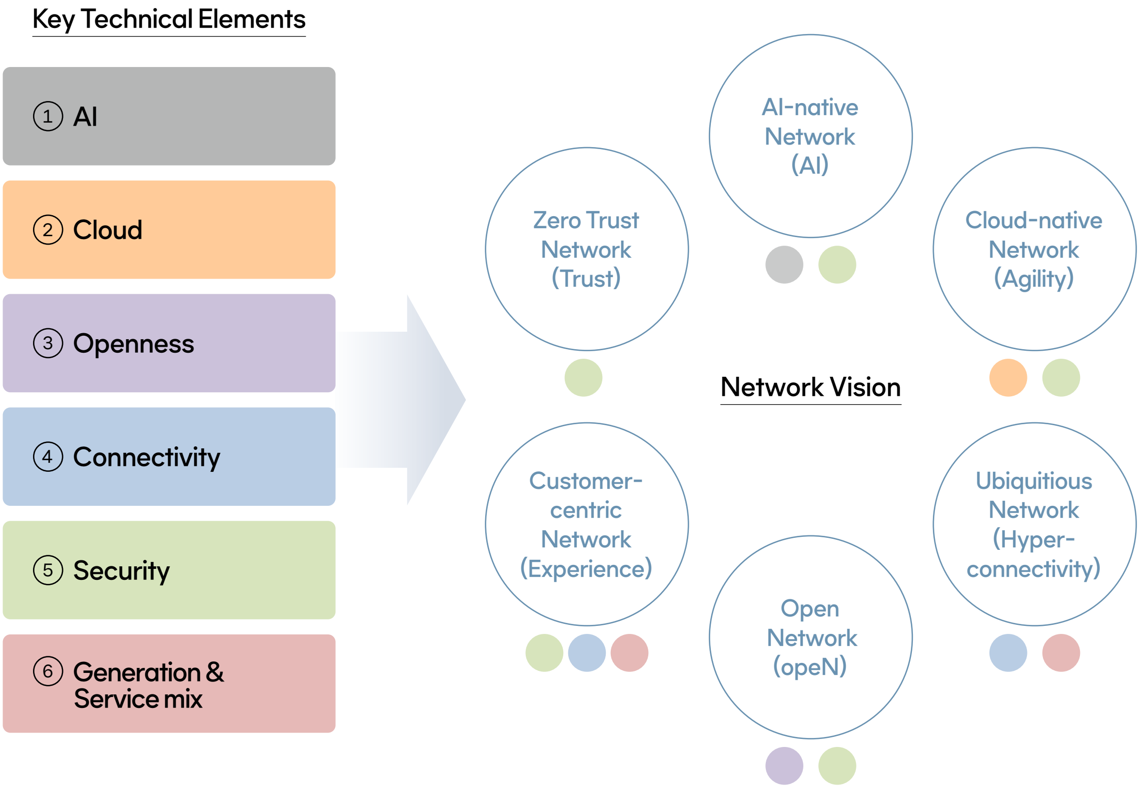
⑥ Convergence of Generations and Services

Following the evolution of mobile communication generations including 3G, 4G, and 5G, 6G is being developed with a service-centric approach rather than a complete generational transition, focusing on flexible architecture design based on coexistence with existing generations and systems. For example, there are active discussions on the development of technologies such as inter-DU pooling technology, which flexibly utilizes base station resources according to time-of-day and regional characteristics, and the simultaneous use of 5G-6G frequencies through MRSS (Multi-RAT Shared Spectrum) to expand mobile network coverage according to generational evolution.

In addition, research is underway to utilize communication resources to support various services such as AI in addition to connectivity support. Discussions are also underway to develop orchestration technology for flexible utilization of network resources to support AI workloads of new 6G services such as AR glass and robot.

2.2 Evolution Direction

SK Telecom has defined six network visions: “AI-native Network (AI)”, “Cloud-native Network (Agility)”, “Ubiquitous Network (Hyper-Connectivity)”, “Open Network (opeN)”, “Zero-Trust Network (Trust)”, “Customer-centric Network (Experience)” [Figure 3].


Key Technical Elements
① AI
② Cloud
③ Openness
④ Connectivity
⑤ Security
⑥ Generation & Service mix
Network Vision
AI-native Network (AI)
Cloud-native Network (Agility)
Ubiquitous Network (Hyper-connectivity)
Open Network (opeN)
Customer-centric Network (Experience)
Zero Trust Network (Trust)

[Figure 3] Mid- to Long-term Network Vision

1. AI-native Network

AI-native network refers to the deep integration of AI technology into the overall operating principles and architecture of the network, evolving along two axes: AI for network and network for AI. From the AI for network perspective, networks will develop into fully intelligent networks that autonomously recognize and optimize situations through real-time data analysis and AI-based decision-making. It minimizes operator intervention and automates operations, performance optimization, failure prediction, and recovery based on Operational Intelligence, maximizing operational efficiency and service agility. Furthermore, it enables differentiated value creation through customized customer services and other innovations.

From the network for AI perspective, networks are designed and optimized to smoothly operate AI services. Evolution toward networks that efficiently support AI workloads by converging computing and communication on telecommunications infrastructure with high-performance and low-latency characteristics is expected. To achieve this, the same hardware should be able to concurrently operate both communication services and AI services, enabling new revenue using the communication infrastructure itself.

2. Cloud-native Network

Cloud-native network means expanding virtualization technology to telecommunications networks, evolving into infrastructure that can flexibly expand or reduce network resources as needed and intelligently redistribute them according to traffic patterns or service characteristics. This enables end-to-end control and operation across all mobile communication domains including radio access networks, core networks, transport networks, and service layers, thereby simultaneously achieving operation automation and optimization while enabling customer experience-centric integrated management.

3. Ubiquitous Network

Ubiquitous network aligns with SK Telecom's 6G strategy of "Generation Mix," meaning evolution toward generation agnostic infrastructure that is not dependent on specific generations such as 5G or 6G and can flexibly distribute and adjust resources according to demand. This enables building networks where existing and next-generation technologies coexist and organically connecting entire networks to provide seamless coverage. Furthermore, when the telecommunication network provides connectivity, it is also possible to provide optimal service-oriented performance and quality that can efficiently provide various services.

4. Open Network

Open network is an open ecosystem that is not tied to a specific vendor by utilizing COTS (Commercial Off-The-Shelf) hardware and open interface-based technologies. This is expected to enable not only TCO reduction but also flexible network operation and, furthermore, facilitate the introduction of AI-based automation and optimization technologies, enabling operator-centric network design. In addition, it is possible to open network-owned data and assets to external parties to create new services and revenue based on Network as a Platform.

However, while aiming for an open network, it is necessary to pursue security through authentication and encryption between network equipment and internal functions. This leads to the following zero trust network vision.

5. Zero Trust Network

The concept of “Zero Trust Architecture”, defined under the principle of “Trust nothing, verify everything”, is a security paradigm that continuously verifies all connections and traffic and controls them with least privilege, which is an essential direction for future networks.

A zero trust network can be defined in conjunction with the other visions above. For example, in an AI-native network, ‘continuous verification’ and ‘automatic threat response’ can be realized by automatically detecting signs of anomalies and dynamically adjusting real-time policies. In a cloud-native network, fine-grained access control and trust verification are applied on a per-microservice and container basis, and the principles of ‘least privilege’ and ‘segmented access control’ are strictly observed even in a distributed infrastructure environment. Additionally, in open network environments, zero trust’s important elements, including authentication for APIs and external access, authorization, and real-time threat monitoring, should be further strengthened for interworking between various systems.

6. Customer-centric Network

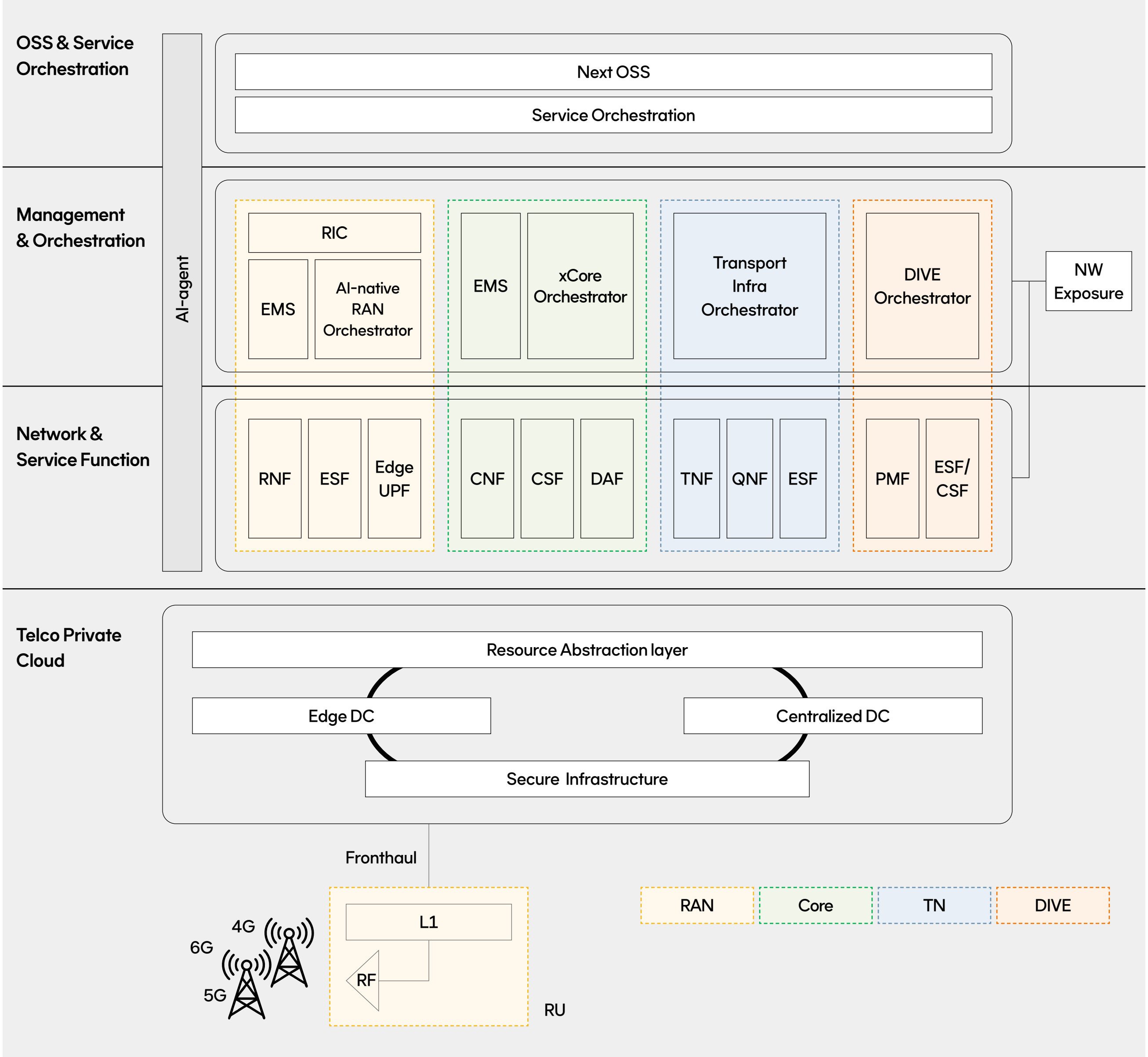
Customer-centric network means designing and operating networks with customer experience and requirements as the top priority, rather than being operator-centric. This approach goes beyond providing stable networks by reducing failure rates close to zero and protecting customer data for trustworthy communication. It aims to maximize customer-perceived service quality by improving key network quality indicators such as data throughput and latency.

In the 6G era, the types of devices utilizing networks, including humanoid robots, autonomous vehicles, and AR glasses, are expected to diversify significantly, and new services with different characteristics, such as Physical AI, are expected to expand. To flexibly prepare for these environmental changes, developing customer-centric network technologies and establishing corresponding operational strategies are required.

2.3 Analysis of Key Technical Elements

In this section, SK Telecom's mid- to long-term network architecture, ATHENA (AI, Trust, Hyper-connectivity, Experience, opeN, Agility), is defined to achieve the network vision presented in Section 2.2. The ATHENA in [Figure 4] is defined in consideration of the radio access network, core network, and transport network domains, as well as the DIVE (Data Insight & Value Engine) to support new functions based on network data.

The design philosophy of the ATHENA architecture shown in [Figure 4] aims to provide an architecture to achieve the network vision defined in [Figure 3].



[Figure 4] ATHENA Architecture

AI-native Network	AI-Agent and leveraging AI as a critical enabling technology to achieve performance improvements across various domains
Cloud-native Network	CNF-based Network Architecture Design & Telco Private Cloud Definition, E2E orchestration
Ubiquitous Network	Domain-specific Orchestration Enhancement for Convergence and Diverse Service Enablement
Open Network	Emphasis on Open Fronthaul and NW exposure, Newly defined DIVE
Zero Trust Network	Considering ZTA as a fundamental element in network architecture and interface design
Customer-centric Network	Maximizing customer-perceived service and network quality, domain-specific orchestration enhancement

Below, we will briefly define the functions of each layer, and describe the details of each domain in the next section.

1. OSS & Service Orchestration

This layer consists of OSS (Operation Supporting System), which supports fault management, performance optimization, configuration management, and service provisioning for stable network operation, and orchestration, which supports integrated control and automation from the perspective of end-to-end networks. Orchestration allocates and coordinates resources across all necessary domains (radio access networks, core networks, transport networks, etc.) in accordance with product/service requirements and policies.

2. Management & Orchestration

Each domain, such as radio access networks, transport networks, and core networks, has different equipment characteristics and technology stacks with high complexity, requiring dedicated management and control of resources and functions within specific domains. Orchestration at this layer supports domain-specific services and functions, enabling optimal resource allocation, fault response, and performance improvement within each domain, thereby securing both operational efficiency and quality simultaneously. Additionally, it supports end-to-end integrated operations by interworking with the service orchestration layer above.

Domain	Function	Explanation
Radio access network	RNF (Radio Network Function)	Resource management and policy control for delivering telco services in the RAN domain - Resource management: Allocating and optimizing radio resources - Policy control: Connections based on resource management information, management policies for packet flow - Packet management function: Create and deliver data packets according to policy rules
	ESF (Edge Service Function)	Specialized services in edge environments
	Edge UPF (Edge User Plane Function)	Distributed UPF for handling user data traffic at the edge - As a concept separate from core network UPF, capable of providing edge-specific functions such as latency reduction.
Core Network	CNF (Core Network Function)	NF (Network Function) providing user mobility management, authentication, session, policy, billing, voice, messaging, and data services
	CSF (Centralized Service Function)	NF providing value-added services
	DAF (Data Analytics Function)	Analytics function that collects and normalizes operational and user data to provide statistics, prediction, and anomaly detection, enabling other NFs to subscribe and query
Transport Network	TNF (Transport Network Function)	Provides L0-L3 transport network functions through software-based virtualization - IP/MPLS Router, IP multicast router - Ethernet switch - L2-L3 VPN router - L3-L7 Load balancer
	QNF (Quantum Network Function)	Provides functions for quantum network management such as quantum encryption and quantum key distribution
	ESF/CSF (Edge/ Centralized Service Function)	Provides xPU training/inference services based on network data
DIVE	PMF (Pipeline Management Function)	As an integrated layer connecting ESF and CSF, automatically configures and manages pipelines among data, processing nodes, AI models, and services
	ESF/CSF	Network data service development, operation, and deployment in edge and cloud domains - ESF: Provides service functions at the edge and interworks with cloud, capable of independent autonomous execution - CSF: Performs integrated management of edge, policy, and operations in the cloud and provides cloud service functions

3. Network & Service Functions

This layer consists of function blocks that provides specific network services such as security, traffic control, and network-based value-added services, and provides key functions for each domain. In the radio access network domain, it considers functions for edge service support as well as basic RAN resource management and policy control. In the core network domain, it includes functions for subscriber management and service provision. In the transport network, it considers functions for efficient transmission and support for quantum network security technologies.

4. Telco Private Cloud

This is the virtualized infrastructure supporting network functions and Telco-based services. Through scalable and efficient hardware and software configurations, SK Telecom is considering the introduction of solutions with enhanced security and scalability.

5. AI Agent

AI agent refers to an autonomous software system or program that uses AI technology to automatically complete tasks on behalf of operators. As an important capability for achieving AI-native network, it can be applied across all domains and layers according to their specific purposes and scenarios. For example, it can analyze traffic patterns and fault situations in real-time and perform resource allocation and fault recovery on behalf of human instructions. It can be utilized for continuously monitoring and predicting QoS (Quality of Service) and QoE (Quality of Experience). Additionally, it can be applied to enhance network security by detecting and responding to abnormal traffic or security threats.

6. Network Exposure

Network exposure refers to the capability of securely providing network status and data to external applications or services through standardized APIs. Through this, external service providers can ensure network-based service quality, while mobile network operators can create new revenue streams. Previously, it was provided mainly for core networks, but with the emergence of the edge AI concept, research is actively underway to support this function in other domains such as radio access networks and DIVE.

In the next section, we will discuss the detailed structure and technologies that should be considered in radio access networks, core networks, transport networks, and DIVE - a new domain based on network data.

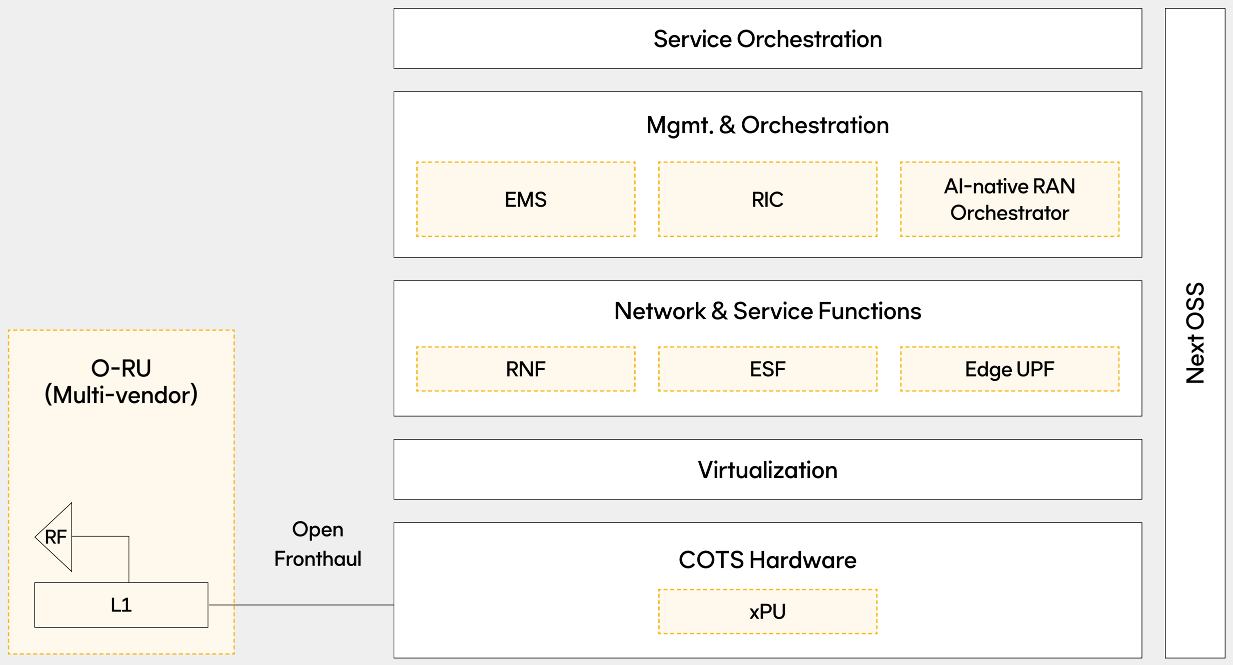
3. Detailed Architecture & Enabling Technologies by Domain

This section presents the detailed architectures of key domain areas in the mid- to long-term network architecture described earlier and describes them in detail from the perspective of implementation technology.

3.1 AI-native RAN (Radio Access Network)

Radio access networks should evolve into AI-native RAN, where the telecommunications network itself combines with AI technology. AI-native RAN has two axes: RAN automation and optimization utilizing AI based on open interfaces and virtualization (AI for RAN), and proactive infrastructure for supporting AI services (RAN for AI). These two axes should be integrated in a mutually complementary relationship. Additionally, it should be designed based on Zero Trust principles that continuously verify all access.
The AI-native RAN architecture is shown in [Figure 5]. Network & Service Functions utilize xPU-based COTS servers and consist of RNF providing existing Telco services and ESF capable of providing AI solutions (independent of telco) or edge services such as autonomous driving control and AR/VR. Also, edge UPF deployment is necessary for efficient traffic processing at the edge. Additionally, it aims for an intelligent network that can optimize the network by collecting and analyzing network and user data in real-time (RIC, RAN Intelligent Controller) and manage it efficiently through AI-native RAN orchestrator.
The following factors should be considered to realize AI-native RAN:

First, through the introduction of xPU-based servers and edge UPF, base stations are redefined as intelligent nodes capable of AI computation, enabling simultaneous provision of communication services and edge services with flexible resource allocation between them.
Second, it should transition to an intent-based intelligent network that minimizes operator intervention, improving performance through self-optimization and enabling efficient management and optimization of resources throughout the entire infrastructure through orchestration.
Third, virtualization is necessary to support the complete decoupling of hardware and software, enabling flexible redeployment of RAN (Radio Access Network) components as needed.
Fourth, equipment should flexibly interwork based on open interfaces and be managed without vendor compatibility constraints, with high-quality, granular, and normalized data acquisition necessary for efficient operation.
Fifth, continuous mutual authentication and traffic encryption between internal equipment functions and across equipment are essential. In addition, security enhancement should be considered even in initial access procedures.



[Figure 5] AI-native RAN Architecture

3.1.1 AI Integration

AI-native RAN should support an architecture that can simultaneously perform existing connection-centric communication services and computing operations for AI services.

General-purpose hardware should be equipped with xPU (GPU, NPU, etc.) to process RAN services and AI services in parallel, and RAN computing and AI computing should be able to share and utilize xPU resources through virtualization between hardware and software. This allows RAN services and AI services to be provided simultaneously in one infrastructure. The AI computing power of AI-native RAN is utilized in two main areas.

First, AI-native RAN can intelligently optimize signal processing in upper layers and physical layers of base stations by utilizing AI computing power. This enhances RAN performance and energy efficiency, enabling evolution toward sustainable communications infrastructure. For example, performance can be improved by applying AI to link adaptation technology that adjusts data transmission parameters according to radio channel conditions based on data such as internal base station information and user equipment reports. Performance and quality can be enhanced through AI-AI (AI-native Air Interface) technology that applies AI to signal processing within the physical layer performing data transmission and reception between base stations and user equipment. Additionally, network energy efficiency can be enhanced by precisely adjusting Energy Saving operations utilizing AI-based traffic pattern prediction results.

Second, AI services from operators or third-party manufacturers can be provided independently from RAN. AI-native RAN can provide infrastructure for low-latency inference-based AI services and AI services requiring high security by forward-deploying AI computing power at the edge. Through this, telecommunications infrastructure can add value through new business models such as edge AI services and network API provision, beyond simple connectivity services. Additionally, for more efficient traffic processing, deploying UPF that delivers and processes user data within AI-native RAN should be considered.

3.1.2 Automation and Optimization

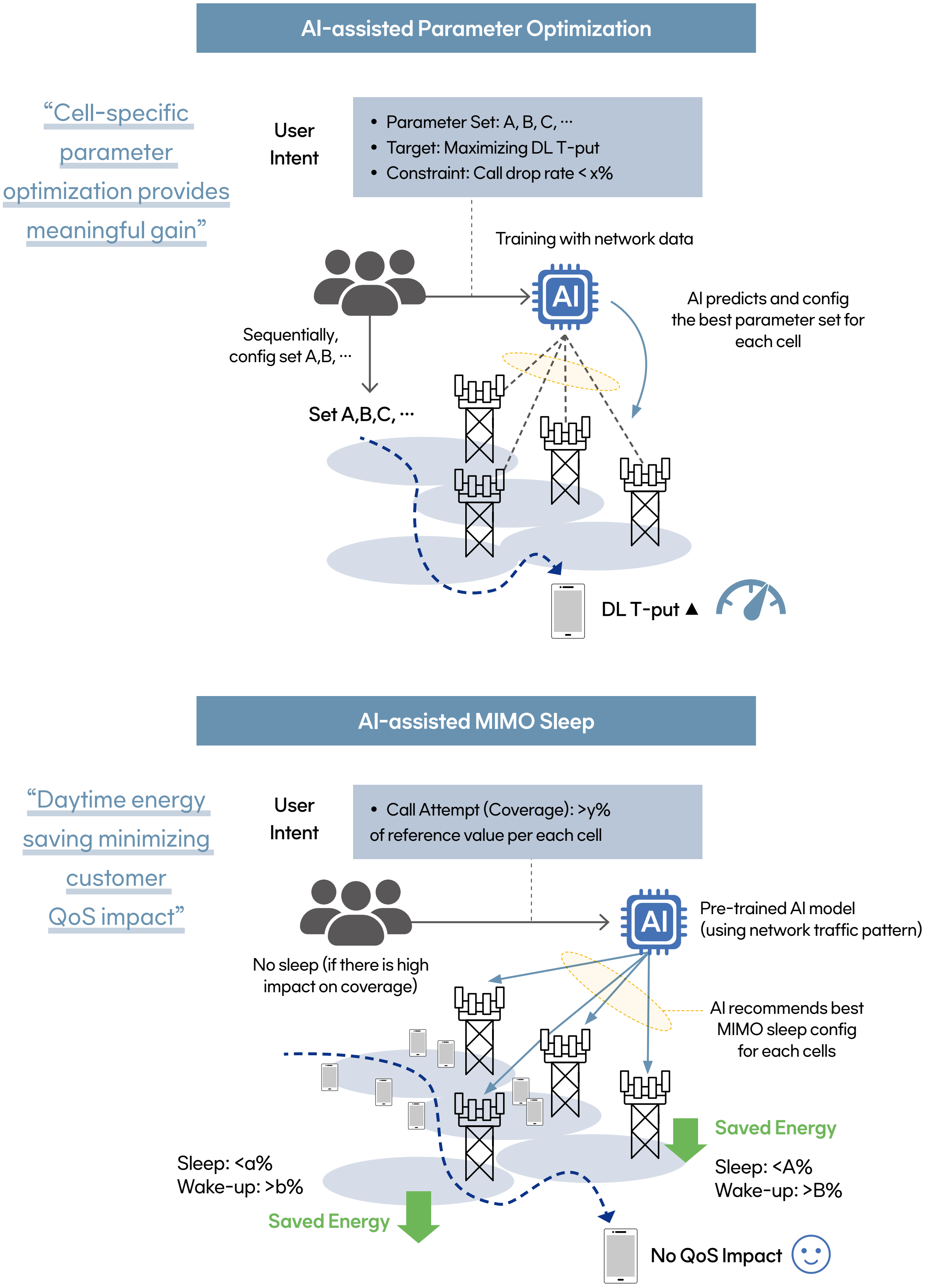
In the future, the network should be composed of an intent-based intelligent network that can minimize the intervention of operators.

AI-native RAN should not only collect and manage various information generated by network infrastructure and user equipment through EMS (Element Management System), but also be able to perform analysis and real-time self-optimization using RIC.

Based on the collected data, RIC uses AI Agent to perform network optimization such as intent-based load balancing, coverage optimization, operation parameter optimization, and energy saving without direct operator intervention. Additionally, each solution operating in RIC is in application form based on open interfaces, enabling equipment manufacturers as well as operators or third-party manufacturers to develop applications reflecting their intent and apply them to networks when necessary.

In order to efficiently manage resources in the operation of virtualization-based AI-native RAN, it is necessary to support AI-native RAN Orchestrator. The AI-native RAN Orchestrator should be able to perform not only resource pooling according to the traffic of each base station, but also orchestration between RNF and ESF to efficiently utilize resources within the same hardware. For example, hardware at times or locations with low traffic can minimize resources for RNF and concentrate on providing resources for ESF operation. Additionally, AI-native RAN Orchestrator should support lifecycle management functions for RNF and ESF.

AI-native RAN inevitably faces a new challenge: hardware heterogeneity. Operators introduce equipment from various vendors at different points in time depending on their network deployment plans. Additionally, differences in performance and functionality occur depending on introduction timing, and this heterogeneity causes complexity throughout the infrastructure, not limited to just central processing units (CPUs) or accelerators (GPUs, NPUs, etc.) but extending to NICS (Network Interface Cards), timing hardware for precise time synchronization, and even cooling systems. Therefore, AI-native RAN Orchestrator should consider integrated orchestration for servers/sites with mixed configurations of different manufacturers and generations and heterogeneous hardware such as CPU/GPU/NPU/DPU.


AI-assisted Parameter Optimization

"Cell-specific parameter optimization provides meaningful gain"
User Intent
• Parameter Set: A, B, C, …
• Target: Maximizing DL T-put
• Constraint: Call drop rate < x%
Training with network data
AI
AI predicts and config the best parameter set for each cell
Sequentially, config set A,B, …
Set A,B,C, …
DL T-put ▲

AI-assisted MIMO Sleep

"Daytime energy saving minimizing customer QoS impact"
User Intent
• Call Attempt (Coverage): >y% of reference value per each cell
AI
Pre-trained AI model (using network traffic pattern)
No sleep (if there is high impact on coverage)
AI recommends best MIMO sleep config for each cells
Saved Energy
Sleep: <A%
Wake-up: >B%
Sleep: <a%
Wake-up: >b%
Saved Energy
No QoS Impact

[Figure 6] RIC Use Case Examples

3.1.3 Virtualization

AI-native RAN should be based on a virtualized base station architecture that enables flexible operation through independent design and configuration of hardware and software.

Existing base stations are designed and configured with manufacturer-specific hardware and software, which may have some constraints in designing and configuring networks according to operator intentions. For example, even if operators want to utilize chipsets such as GPUs or NPUs to add AI computing, it is difficult to reconfigure dedicated hardware according to operator intentions.

In contrast, AI-native RAN can configure xPU in general-purpose servers without specific structural constraints as needed and simultaneously operate RNF providing RAN services and ESF providing AI services or edge-based specialized services according to operator purposes through virtualization.

Additionally, AI-native RAN should support technologies that can leverage virtualization advantages such as resource pooling technology. For example, operators can optimize total power consumption by reducing the number of operating servers through scale-in technology when traffic load is low in a virtualized environment. Conversely, when traffic load is concentrated, cell capacity and stability can be increased without disrupting service by utilizing technologies such as scale-up or cell pooling.

Finally, AI-native RAN should be able to flexibly operate and utilize the network by taking advantage of virtualization. Since hardware and software can operate independently, operators can provide 4G, 5G, and even 6G services independently or simultaneously on a single hardware platform. Alternatively, operation efficiency could be maximized through resource sharing and allocation between services according to demand while simultaneously providing RAN services and AI services.

3.1.4 Open Interface

AI-native RAN should aim for interface openness to improve flexibility and cost efficiency, requiring the introduction of open interfaces based on standards such as those from the O-RAN Alliance.

O-RAN is an infrastructure architecture that standardizes interfaces between equipment and within equipment to enable interworking of equipment from different manufacturers. The O-RAN Alliance was established in 2018 to discuss related standardization and is advancing standardization of inter-equipment and intra-equipment interfaces.

AI-native RAN introduces these standardized interfaces to interwork equipment or solutions from different manufacturers, and operators should be able to achieve integrated control of heterogeneous manufacturer equipment through this approach. As intra-equipment interfaces are also implemented as open interfaces, interworking and operation between heterogeneous manufacturers become possible at the software level. For example, even when RNF and ESF from different manufacturers operate within the same hardware, monitoring and control are possible based on standard specifications. Additionally, EMS and base stations should interwork based on open interfaces, enabling equipment connection and data collection without manufacturer-specific constraints between equipment manufacturers. Each solution operating in RIC takes the form of AI applications and is implemented based on open interfaces, so not only equipment manufacturers but also operators can develop applications reflecting their intent and apply them to the network.

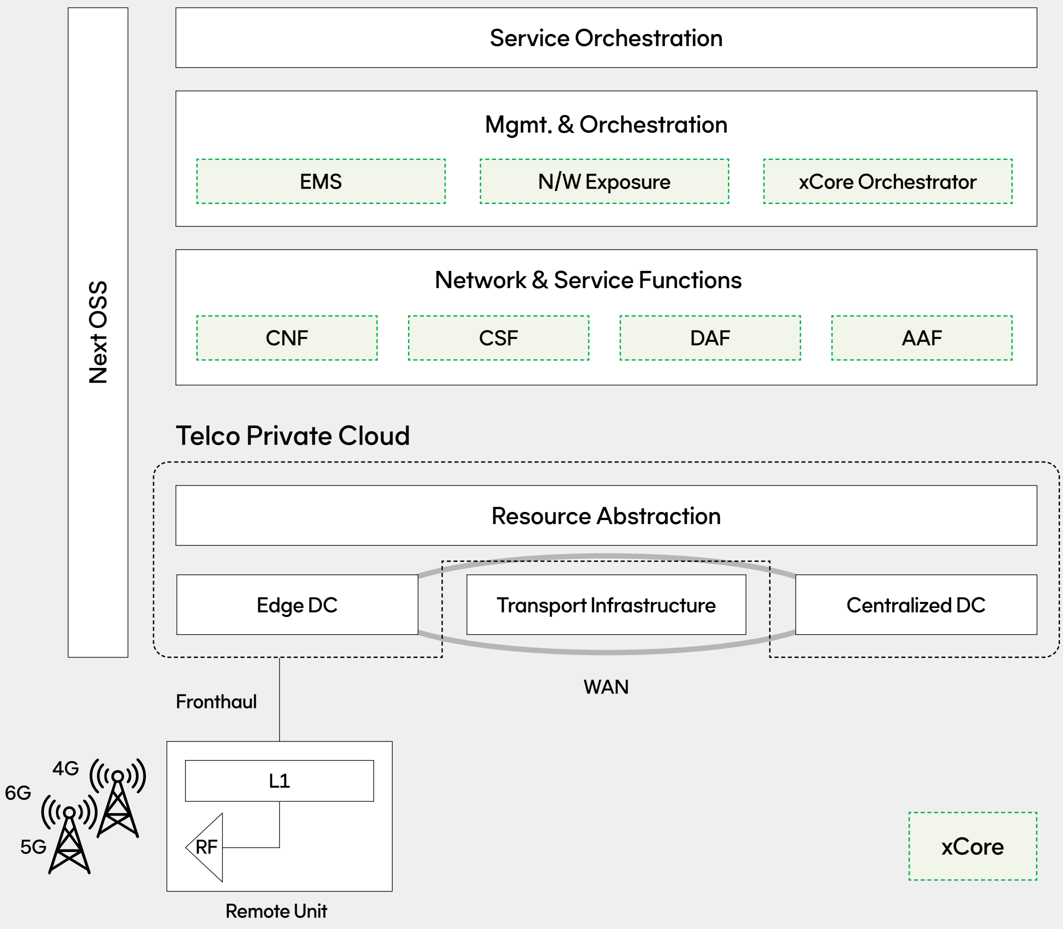
In other words, AI-native RAN enables flexible network deployment and cost efficiency by diversifying equipment lineups based on open interfaces, and should support AI agent-based operation and optimization without manufacturer dependency. Additionally, to realize this, high-quality, granular, and normalized network and user equipment data should be secured based on open interfaces without constraints between heterogeneous manufacturers. For example, not only simple cell-based data but also granular data such as equipment-specific data such as repeaters constituting cells or service-specific data should be normalized and extracted without on-site measurements. Additionally, such data can be provided through Network Exposure, and the provided data can be used by NWDAF (Network Data Analytics Function) for RAN analytics, by operators' OSS, or by third-party service providers to monitor performance or for AI/ML training.

3.1.5 Zero Trust Architecture

AI-native RAN should aim for ZTA that inherently trusts no entity or network and always verifies. Because existing networks trusted internal data or equipment to a certain level through perimeter-based security models, it is necessary to be prepared for insider intrusions and increasingly sophisticated hacking attacks. ZTA should be applied to perform continuous verification and encryption for all user, equipment, and application access. Operators and manufacturers are applying Zero Trust philosophy to infrastructure through implementing their own security solutions, and related standardization is being actively discussed in standards bodies such as the O-RAN Alliance.

For AI-native RAN to support ZTA, access identification and management need to be strengthened through encryption mechanisms that are scalable across large-scale network environments. Additionally, continuous monitoring of attacks and policy automation are necessary. Through this, abnormal signs can be detected in real-time based on AI and security policies can be dynamically adjusted. Furthermore, resource and workload isolation should be strengthened to prevent the breach propagation that can occur in virtualized environments. Finally, balance between security and performance should be maintained when applying ZTA. For example, for latency-sensitive services such as XR, real-time industrial control, and V2X that can be provided at the edge, optimization is necessary to ensure ZTA implementation does not negatively impact service quality.

3.2 xCore



[Figure 7] xCore Architecture

3.2.1 AI-native Core

The core network serves as a central gateway connecting voice and data traffic generated from numerous customer terminals to the internet and service domains. Through the core network, various control and user plane functions such as terminal access, authentication, registration, address allocation, handover, QoS policy, session management, and billing processing are integrated and separated, consisting of cloud-native-based NF, SF (Service Function), and DAF (Data Analytics Function) responsible for service continuity, policy enforcement, billing processing, and analysis [Figure 7]. Future core networks are expected to evolve in the direction of the Beyond Connectivity concept, moving beyond simple connectivity to encompass AI, Computing, and Zero Trust Security. To accommodate

this, the protocol interworking structure between terminals and networks should be simplified as much as possible, and communication efficiency between NFs should be dramatically improved. For example, future core networks are expected to enhance operational efficiency by reducing hierarchical structures or interworking dependencies compared to current ones and natively integrating intelligent functions including AI into each NF. From 2025, discussions on core 3GPP 6G standard technologies will intensify, with AI/ML, SBA (Service Based Architecture), Computing, data processing, and new security frameworks expected to be reflected in standards.
Future core networks are expected to undergo functional expansion and evolution based on 'AI Agentic Function (AAF)' and should be capable of various real-time data analysis, learning, and inference utilizing DAF. To realize this, the following implementation elements should be considered:

① To achieve service TTM (Time-to-Market) and Operational Efficiency, an intent-based operation system should be introduced where operators only set goals (e.g., latency, availability, cost limits, etc.) and agents establish plans by domain, applying and executing them per service.

② A collaboration system among various monitoring, diagnosis, quality, security, and service agents should be established to enable mutual exchange and optimized scenario execution.

③ A reliable closed-loop should be established that pre-verifies NF changes utilizing Network Digital Twin technology, reduces failure rates through Canary Update and Rolling Upgrade, and secures high confidence in prediction results.

④ Root cause analysis, recurrence prevention, and proactive prevention should be systematized through domain knowledge data-based operations combining logs, metrics, and policies.

⑤ Network capabilities such as QoS, security, location, and events should be provided as productized Open APIs, incorporating usage-based revenue models to expand the market from a Network-as-a-Platform perspective.

Based on these changes and innovations, core networks should achieve evolution toward AI-native Core, progressing from gradual automation to complete autonomous operation.

3.2.2 Cloud-native

Future core networks are expected to evolve into a complete CNF (Cloud-native NF) environment, where all network functions are implemented based on MSA (Micro Service Architecture) and can be flexibly ported and deployed across multi/hybrid clouds. Additionally, gradual evolution is necessary toward functional granularization and integrated operation for stable management of generation-specific networks, verified quality, increased development speed, improved investment efficiency, and simplified management. This structural evolution is expected to bring innovation in multiple aspects, including not only network design simplification but also operational and capital expenditure reduction and rapid new service provision.

Furthermore, AI enables NF resource optimization, power savings, and CI/CD (Continuous Integration/Continuous Delivery, Deployment) policy-based operation, allowing self-healing and in-service SW upgrade capabilities. AI constantly monitors NF operation to detect abnormal behavior in advance and execute measures. For example, when an AI model predicts failure signs, the core network itself performs procedures to change traffic paths or isolate and recover defective NFs without human intervention. As a result, a Robust and Resilient Core Network is expected to be realized where entire services do not stop due to a single failure, like a "core network that doesn't die even when it dies." This ultimate goal is to achieve optimal availability without operator intervention, and technologies and standards are expected to develop toward building and operating core networks with stability at the level of fully autonomous networks (e.g., Level-4 autonomous networks).

Orchestration of future core networks dynamically deploys and manages communication functions in hierarchical computing environments spanning cloud, edge, and terminals by analyzing network conditions and various service requirements in real-time based on AI/ML to automate optimal resource placement and traffic routing. Additionally, through intent-based networking, operators' intent is automatically converted into network policies, guaranteeing seamless service continuity without quality degradation. In 6G, operational efficiency is expected to be maximized through these automation capabilities.

3.2.3 Service Enabling Technology

Network Exposure services can be described as the stage of "open network utilization through standard/Open APIs." Future core networks are expected to evolve beyond simple API calls to Context-aware Exposure (exposure reflecting user situations/environments) and Intent-based Exposure (where networks automatically provide services by translating service intent into policies), evolving into operator Monetization solutions through new Business Models.

Roaming Edge services build cloud-based data processing UPF in global regions with a structure controllable from the Home network, providing data traffic at the closest distance to customers roaming abroad. Future core networks are expected to evolve into service-oriented network providing global connectivity without border restrictions by applying not only network resource Isolation and QoS guarantees for various granular Slices but also AI and Computing functions to users such as vehicles and robots.

3.2.4 Zero Trust Architecture

Core networks handle customer access, authentication, and billing and, therefore, It is imperative to introduce more advanced and stringent security technologies because they interact with numerous distributed equipment while processing various sensitive data. For example, areas utilizing older protocols should be given particular attention. Additionally, various sophisticated defense solutions are needed for malicious penetration and hacking (detection of fraudulent SIM/terminals, spam, and Fake base station attacks).

In future core networks, NEF (Network Exposure Function) and API Gateway are important for network openness and service expansion, but they are one of the major security vulnerability points where external attacks and internal threats intersect, making it difficult to respond to complex threats with the existing perimeter security-centric model. Accordingly, a Zero Trust-based approach is necessary that continuously evaluates all API calls and data flows and dynamically defends. At this time, various factors including request origin, certificate validity, message integrity, and token expiration should be verified each time API traffic reaches the gateway. Even during sessions, the ability to continuously check the access subject's state and behavior patterns, identify abnormal signs, and discontinue access when necessary is required.

Access rights should be granted based on the principle of least privilege, only within the scope absolutely necessary for the calling subject, and authorization scope should be granularized to the API endpoint level. Additionally, all data transmission sections should use encryption through the latest IPSec and TLS (Transport Layer Security) specifications as default, with end-to-end encryption and integrity verification required.

Vulnerabilities within core networks require constant inspection and action, with improvements needed according to international mobile telecommunications security guides (e.g., GSMA FASG). Particularly, systematic advancement is necessary to secure security and resilience across all core network sections through telco security governance by continuously reflecting 1) software supply chain security enhancement, 2) communication/storage encryption and algorithm strengthening, and 3) Micro Segmentation based on closed-loop (e.g., configuration parameters).

Future core networks are expected to dramatically improve security levels across telecommunications infrastructure by automatically and continuously analyzing security vulnerabilities through AI and continuously reflecting improvements.

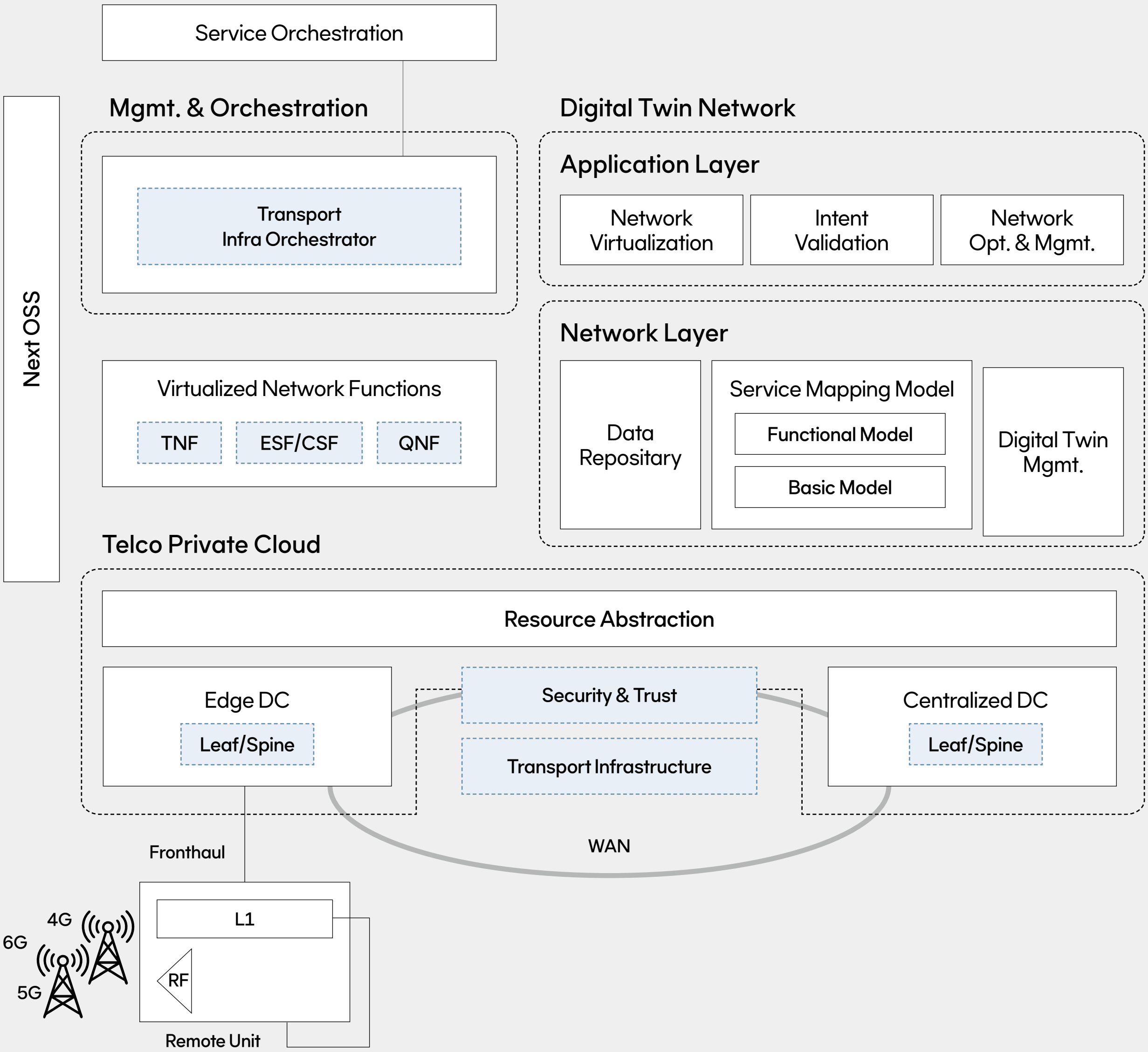
3.2.5 Centralized DC

SK Telecom's Centralized DC continues to evolve as an AI data center (AI DC), performing roles as central management, control, and intelligent hub for core network functions. It implements intelligent closed-loop-based control by centralizing major core NFs such as NWDAF performing AI and structurally linking them. Through AI Orchestrator and SDI (Software-Defined Infrastructure), automatic construction, scaling, and operation of resources become possible, dramatically improving core network resource management efficiency and response speed. Through NWDAF, signals and data collected from distributed NFs can be analyzed to predict and detect abnormal equipment operation, traffic congestion, etc., performing network performance optimization. Additionally, network functions are exposed externally through standardized APIs to enhance service interoperability, and by introducing various intent-based controls to automatically reflect operators' intent in network policies, core network operation autonomy is further strengthened. Through these development directions, evolution toward an AI-native Core structure centered on centralized data centers is expected.

3.3 ACTN (AI-native Converged Transport Network)

AI-native Converged TN is the transport network infrastructure for SK Telecom's future transport network innovation, evolving with goals of network intelligence and autonomy, security enhancement, operational automation, and improved scalability and cost-efficiency. AI-native TN is developing into a network that internalizes operator experience and expertise in AI through AI-based integrated control and management systems, realizing intelligent operations such as real-time resource allocation, failure prediction, and traffic optimization. This intelligent operation, combined with APN-based structural evolution and the introduction of next-generation optical transmission technologies such as Layer 0~3 Converged equipment, Open API, and Next-Generation Reconfigurable Optical Add-Drop Multiplexer (NG-ROADM), maximizes network architecture simplification, flexibility, scalability, and cost-efficiency. Network openness and standardized interfaces enhance operational efficiency in Multi-Vendor environments and provide a foundation where various equipment and services can organically interwork.

From a security perspective, data transmission security is innovatively enhanced through a dual security structure combining quantum cryptographic communication (QKD) and PQC (Post-Quantum Cryptography), API-based automation, and real-time detection and response systems. This enables End-to-End security realization not only in data centers and B2B sections but also in various network environments such as Edge, IoT, and backhaul. Additionally, to enhance network reliability and stability, a Digital Twin environment is built to precisely virtualize actual transport networks, realizing an intelligent



[Figure 8] AI-native Converged TN Architecture

network operation system capable of operational simulation, automation, optimization, prediction, and verification. Digital Twin provides a foundation for safely performing various operational tasks such as new service design, failure response, quality diagnosis, and resource optimization.

To respond to the AI era, large-scale AI training and inference services are supported by linking AI DCs with nationwide central office clusters based on xPU-based DCI (Data Center Interconnect) transport networks. By applying open equipment and SDN-based integrated control, resource optimization and operational efficiency are maximized, implementing a network architecture that can flexibly expand and contract according to service demand and traffic changes. This infrastructure realizes goals of network intelligence and autonomy, security enhancement, operational automation, and improved scalability and cost-efficiency through organic interworking of each element including AI-native RAN, Digital Twin, and quantum cryptographic communication.

Through the evolution of AI-native Converged TN, SK Telecom can lead the paradigm of future transport networks and plans to provide customers with differentiated network experiences and continuous competitive advantage enhancement.

3.3.1 AI-based Transport Network Integrated E2E Control/Management

based transport network integrated E2E control and management is a core strategy pursued to realize future transport network innovation and intelligent networks. Operator Knowledge-based AI-assisted operation, AI-based automated LCM integrated operation, and Time-scheduling-based E2E xPU Clustering capabilities become the center of next-generation transport network operation systems.

Operator Knowledge-based AI-assisted operation capability internalizes operator experience and expertise accumulated over long periods into AI models, supporting real-time decision-making and automated responses throughout network operations. This enables experience-based decision-making, intelligent failure prediction and response, operational efficiency enhancement, and continuous learning and optimization. AI learns from operator feedback and actual operational data, greatly improving the speed, accuracy, and stability of network operations.

AI-based automated LCM integrated operation capability automates lifecycle management processes including network resource introduction, deployment, operation, and decommissioning. By having AI present optimal operational policies at each stage—including resource introduction and deployment, operation and quality management, decommissioning and recovery, and real-time policy proposals—network stability and quality can be continuously maintained while minimizing operator intervention.

Time-scheduling-based E2E xPU Clustering capability configures clusters by major nodes within the network and dynamically allocates xPU resources within each cluster according to service characteristics and traffic patterns. AI analyzes real-time traffic predictions and service requirements to establish resource allocation plans on an hourly basis, securing network stability and scalability through inter-cluster interworking and load balancing, and real-time monitoring and failure response.

Thus, the AI-based transport network integrated E2E control and management system provides the foundation for future transport networks to evolve intelligently and autonomously, becoming a core driver for providing differentiated network experiences to customers and continuous competitive advantage enhancement.

3.3.2 APN-based Transport Network Architecture Evolution

SK Telecom is pursuing transport network architecture evolution based on APN (All Photonic Network) with the goal of realizing future intelligent networks. To achieve this, the company is moving away from the existing closed and manufacturer-dependent network architecture, focusing on introducing Layer 0~3 Converged equipment, integrated control and management based on Open API and Open hardware, and simplifying and improving efficiency of the backbone network utilizing next-generation optical transmission technologies such as NG-ROADM. Through these strategies, manufacturer dependency is reduced while dramatically enhancing network flexibility, scalability, and cost-efficiency.

The evolution of APN-based transport network architecture centers on migration to Layer 0~3 Converged equipment. Through the introduction of convergence equipment such as POTN (Packet Optical Transport Network), service-specific path control becomes possible and network architecture is further simplified. Additionally, in the NG-Fronthaul (T-PON) architecture, combining Optical Fiber-based L0 Transparent architecture with PON and tunable optical module technology strengthens network stability and enables various effects including TCO reduction and operational efficiency improvement. Furthermore, in the Open PON architecture, cost-efficiency is enhanced through White Box implementation (pOLT), low-cost CPUs, and L3 Switch removal, implementing a Flexible Network capable of flexibly creating and deleting control, management, and value-added service functions.

Such network architecture innovation also contributes to realizing manufacturer-independent integrated control and management through support for various Open APIs. By applying a Common Management Data Model, various equipment such as IP/MPLS routers, Open hardware switches, and Open ROADM can be managed in an integrated manner, particularly maximizing operational efficiency in Multi-Vendor environments. By utilizing standardized interfaces and data Model-based Open APIs to comprehensively control and manage Open ROADM, both operational efficiency and scalability of the network are secured.

NG-ROADM can realize backbone network simplification and efficiency improvement by applying high-capacity transmission of 200Gbps or higher and CDC (Color-less, Direction-less, Contention-less) technology. Flexible Photonics technology maximizes transmission capacity and spectral efficiency, and software-based dynamic control enhances operational efficiency. Additionally, Open NG-ROADM enables integrated management based on standardized data Models and Open APIs, enabling rapid response to failure situations and service expansion.

As wireless service capacity increases, fronthaul line capacity is also showing a trend of expansion from the existing 25Gbps to 50Gbps or higher. Since Dispersion penalty occurring in optical transmission increases rapidly according to transmission speed, application of modulation methods capable of addressing this is essential in high-speed transmission. Current optical transmission standards use Non-Return to Zero method up to 25Gbps for a single wavelength, and utilize PAM4 (Pulse Amplitude

Modulation 4-level) and DCO (Digital Coherent Optics) technologies at 50Gbps or 100Gbps and above[6].

Existing fronthaul networks have been configured as fixed WDM networks and used without changing network configuration during operation. However, next-generation mobile fronthaul networks possess capabilities to flexibly change network configuration for wireless system resource optimization or energy savings according to user traffic.

Thus, based on network innovation strategies including APN-based architectural evolution, Open router and optical module integrated control and management, backbone network innovation through Open NG-ROADM, and elimination of vendor dependency, SK Telecom is leading the advancement toward intelligence and autonomy in future transport networks.

3.3.3 Quantum Cryptographic Communication Service Provision

As digital transformation and data-centric services such as AI, cloud, and big data explosively increase, the security importance of data transmission through transport networks is significantly highlighted. Particularly with the advancement of quantum computing, awareness is spreading that existing encryption technologies alone cannot perfectly respond to large-capacity, high-value data transmission between DC (Data Centers) and B2B sites in real-time. Accordingly, strategies are being pursued to innovatively enhance security levels of data transmission between DC and B2B sites by introducing next-generation encryption technologies such as quantum cryptographic communication (QKD) and PQC (Post-Quantum Cryptography) into transport networks.

QKD infrastructure distributes quantum keys in real-time based on optical fiber by installing QKD equipment at major points (DC, B2B sites, central offices, etc.), simultaneously supporting encryption key distribution and data transmission encryption by interworking with existing transport networks (OTN, DWDM, etc.). Quantum keys are periodically renewed and utilized as session keys used for data encryption. Additionally, encryption equipment equipped with PQC algorithms is deployed in transmission sections (DC-DC, DC-B2B, B2B-B2B) to ensure security even in quantum computer environments while maintaining compatibility with existing networks. A dual security structure is implemented by combining quantum keys distributed by QKD with PQC algorithms.

QNF (Quantum Network Function) provides functions for quantum network management such as quantum encryption and quantum key distribution. Based on QNF, generation, distribution, renewal, and disposal of quantum keys and PQC keys are automated through QKMS (Quantum Key Management System)and Multi Factor Security, and real-time key exchange and operational automation between various network equipment and encryption devices are realized through API-based interworking. Real-time detection and response systems are also established for key leakage, eavesdropping attempts, and abnormal sign occurrences.

Encrypted transmission combining QKD and PQC is provided for large-capacity data synchronization, backup, and AI training data transmission between mega DCs and regional DCs, and quantum/PQC-based encryption services are also applied to dedicated lines for B2B customers in finance, healthcare, public, and manufacturing sectors. Data confidentiality, integrity, and availability can be guaranteed in various B2B scenarios such as inter-enterprise data linkage, cloud connectivity, and remote backup.

In the future, plans continue to evolve transport network security by expanding End-to-End encryption application scope to Edge, IoT, 5G/6G backhaul, etc., and through operational automation and AI-based security enhancement, Open API and standardization interworking, and customized security services for customers.

3.3.4 DCI Transport Network Configuration for xPU-based Services

In preparation for the full-fledged arrival of the AI era, construction of xPU Clustering-based transport networks linking AI DC (AI data centers) and nationwide central offices is being prepared to provide large-scale data processing and ultra-low latency services. Next-generation network infrastructure is being designed to maximize AI service efficiency and scalability by dividing roles with AI DC dedicated to AI training and nationwide central office clusters dedicated to AI inference.

AI DC provides an environment optimized for AI model training using vast amounts of data by concentrating deployment of high-performance xPU resources such as large-scale GPUs, TPUs, and FPGAs. Operated as ultra-large hubs equipped with advanced cooling, power, and security facilities, it intensively performs high-value-added AI operations such as training the latest AI models, fine-tuning, and large-scale data preprocessing and verification. Various xPU resources such as CPUs, GPUs, and FPGAs are deployed in cluster form at nationwide central offices to provide AI inference services in real-time and low-latency. Central office clusters can rapidly process various AI inference services such as video analysis, voice recognition, and IoT data processing at locations close to customers.

Central office-level xPU clusters secure standardized interfaces, operational automation, and scalability by introducing open equipment (White Box Switch, Open Router, Open ROADM, etc.). By applying Layer 0~3 Converged equipment and SDN-based integrated control (OpenConfig, NETCONF, gRPC, etc.), redundant equipment and complex paths by network layer are minimized, maximizing resource optimization and operational efficiency. Cluster architecture is modularized to enable flexible expansion and contraction of xPU resources and network equipment according to service demand and traffic changes.

When linking AI DC and central office clusters, LCM for AI models is systematically performed. Based on ESF (Edge Service Function)/CSF (Centralized Service Function) providing xPU training/inference functions based on network data, AI models trained and verified at AI DC are deployed to central office clusters, and data and feedback generated during real-time inference services are transmitted back to AI DC for utilization in model retraining and advancement. DCI transport networks rapidly interwork large-capacity model files, data, and feedback information, and when traffic surges or failures occur at central office clusters, load balancing and automatic recovery are possible through linkage with adjacent central offices or AI DC. Central office clusters are linked with various future services such as Edge Cloud, B2B specialized services, and IoT to realize region-specific specialized services and ultra-low latency AI inference.

Thus, next-generation transport network infrastructure optimized for the AI era will be pioneered through Hybrid configuration of AI DC and nationwide central office clusters, open equipment-based xPU Clusters, and systematic model management and service linkage strategies.

3.3.5 Network Digital Twin Environment Provision

Network Digital Twin aims for a next-generation virtualized service environment where all elements of actual transport networks—including structure, resources, traffic, failures, and operational policies—are precisely replicated in digital space, enabling network operational simulation, automation, optimization, prediction, and verification. Through this, a foundation is being established for innovative automation of complex transport network operational tasks and enhancement of network stability, reliability, and scalability.

The Digital Twin environment is designed based on TNF (Transport Network Function), which provides transport network functions in software-based virtualization form, to enable real-time status monitoring and simulation of various operational scenarios by virtualizing all components of actual transport networks—including equipment, lines, paths, services, and traffic flows—into digital models. The goal is to build a precise virtual network at the same level as actual networks by interworking vast operational data including resources and operational policies across Layer 0~3, failure histories, quality data, and traffic patterns. Through this, various operational scenarios such as network architecture changes, new equipment introduction, line expansion/deletion, and service path changes can be verified in advance, minimizing operational risks.

Additionally, the Digital Twin environment is utilized as core infrastructure for network simulation and operational automation. Complex operational situations such as large-scale traffic changes, failure occurrences, new service launches, path optimization, and resource redeployment can be simulated in advance in virtual networks to analyze impacts on actual networks and derive optimal response measures. By automating various operational tasks such as AI-based operational policies, automatic failure response, traffic prediction and resource allocation, and quality diagnosis in the Digital Twin

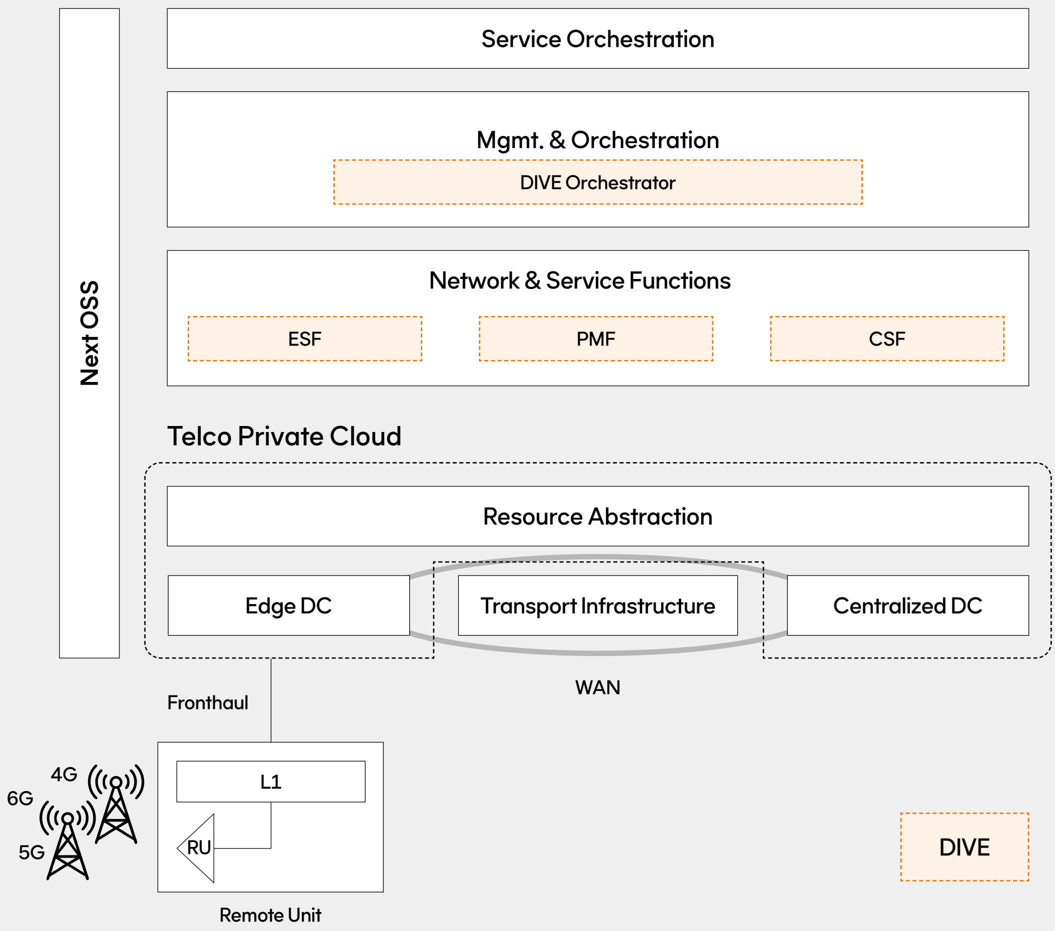
environment, operator workload can be reduced while enhancing network stability and reliability.
Along with this, based on the Digital Twin environment, operators can safely perform various operational tasks such as new service design, failure response scenario verification, quality diagnosis, resource optimization, and policy changes in virtual networks identical to actual networks. When introducing new equipment, equipment interworking tests, traffic flow analysis, and failure possibility verification can be performed in advance to minimize impacts on actual networks. When large-scale traffic changes or failures occur, various response scenarios can be simulated to derive optimal recovery paths and resource allocation policies. Thus, the Network Digital Twin environment is the core foundation of future transport network operation that minimizes operational risks and continuously maintains network quality and stability.

3.4 DIVE (network Data Insight & Value Engine)

As the importance of AI and data rapidly emerges, the mobile telecommunications industry is reexamining vast network data generated from network equipment as a core asset for creating differentiated value beyond basic operational functions. SK Telecom has successfully launched services such as real-time floating population analysis, positioning services, and commercial district analysis solutions by utilizing this data. Additionally, network optimization through base station traffic and field pattern analysis can improve operational efficiency, demonstrating that network data is a strategic asset rather than merely a byproduct.

In the future 6G era, network data utilization is expected to become much more extensive and sophisticated along with advancement in the future network technologies mentioned earlier. Through this, future networks will support various services such as precise indoor location-based services, AI-based network quality prediction and guarantee, Digital Twin-based city management, and industry-specific specialized data services, becoming deeply integrated into industrial sectors.

To effectively create and operate these network data-based services in the 6G era, independent system architectures for each service have clear limitations. Building independent data Pipelines and analytical infrastructure for each service causes issues including redundant development expenditure, increased operational complexity, and delayed new service launches. Additionally, operational challenges such as maintaining security policy consistency and rapid response when failures occur are particularly significant[7].



[Figure 9] DIVE Architecture

Accordingly, this section presents 'DIVE (network Data Insight & Value Engine)', an integrated platform for creating network data-based services in the 6G era. DIVE is a platform that systematically collects, processes, and analyzes various data from network equipment to create new business value. DIVE has core design principles of Hybrid Edge-Cloud architecture, AI-based network data service development and operation environment, Dual Plane deployment separating policy and service deployment, and Zero Trust Architecture, aiming to simultaneously achieve operational efficiency maximization, customer experience innovation, and network-based Monetization.

3.4.1 Hybrid Edge-Cloud Architecture

Network data services in 6G have limitations from perspectives of real-time responsiveness, data transmission costs, and customer data restriction demands with centralized cloud processing alone, and consistent policies and large-scale data analysis are difficult with Edge-based distributed structures alone. DIVE can solve this dilemma through a Hybrid Edge-Cloud architecture combining the advantages of both Edge and Cloud.

The Hybrid Edge-Cloud architecture consists of three core components: ESF (Edge Service Function), CSF (Centralized Service Function), and PMF (Pipeline Management Function). ESF is an execution engine at the Edge that can operate independently in environments such as B2B customer-dedicated networks, collects data from field network equipment, and provides real-time services. ESF operates autonomously, enabling independent service provision based on local policies even during temporary disconnection from the cloud. This is essential in Mission-Critical environments such as factory automation and telemedicine. Additionally, ESF can process and filter network data at the Edge to optimize data transmitted to the cloud, thereby reducing network costs and decreasing processing load in the cloud. It is implemented as a lightweight containerized environment, it enables consistent deployment and execution on various Edge hardware. Additionally, for sensitive or confidential data, Federated Learning techniques can be supported to maintain AI model training effectiveness while preventing data leakage from the Edge.

CSF is an execution engine in the cloud responsible for integrated monitoring of entire network data, policy management, large-scale data analysis, and AI model training. CSF integrates management of policies, service configurations, and operational rules for all Edge nodes by version through a Git-based IaC (Infrastructure as Code) approach. This enables batch deployment or Canary deployment of policies to Edge sites [8]. Additionally, CSF performs analysis of data transmitted from the Edge, Anomaly Detection, and service model training. Trained models are deployed back to the Edge to be utilized for real-time inference in the field. Additionally, by integrating management of all data access histories, policy change histories, and automatic action execution records in the cloud, regulatory requirements such as GDPR and telecommunications network laws can be satisfied, and cross-domain analysis can be performed to discover correlations between different industries or regions and identify new service opportunities.

PMF is an integrated layer connecting ESF and CSF that automatically configures and manages services by establishing Pipelines among data, processing nodes, AI models, and services according to requirements. PMF automatically generates necessary data source identification, preprocessing node selection, AI model mapping, and result delivery paths according to service requirements. For example, when requesting a ‘real-time floating population prediction for a specific area’ service, PMF automatically configures a Pipeline connecting access logs from base stations in that area, movement pattern analysis models, and visualization dashboards. Additionally, service Pipelines are defined as declarative configuration files, and components such as data connectors, preprocessing functions, AI models, and output handlers are registered in component catalogs with standardized interfaces for reusability. PMF dynamically determines whether to execute each stage of the Pipeline at the Edge or Cloud according to service characteristics and resource availability, optimally distributing workloads considering network conditions and Edge resource availability.

3.4.2 AI-powered Data Service Development

DIVE is a platform that can transform network data into services. When service planners propose new service ideas, natural language processing technology analyzes service requirement documents and automatically derives necessary data attributes. For example, for a network congestion prediction service by time zone in a specific region, keywords such as region, time zone, and congestion are extracted, and related network logs including base station access logs, traffic measurement logs, and wireless signal quality logs are identified. Through data catalogs and metadata management systems, highly relevant data is rapidly identified from large-scale data sources.

Extracted data is transformed into forms suitable for AI model training through Feature Engineering Pipelines. Preprocessing tasks such as missing value handling, outlier removal, normalization, categorical variable encoding, and time window aggregation are automatically performed, and results are stored in Feature Stores and managed in reusable forms. Additionally, automated learning model generation technology is utilized to experiment with various Feature combinations and automatically select the most suitable Feature Set for service purposes. Once Features are prepared, the training model generation framework automatically experiments with various AI algorithms and performs hyperparameter tuning to derive optimal models. Model performance is evaluated through cross-validation, and optimal models are managed by version in the Model Registry, tested and validated in actual service environments through A/B testing, and then deployed.

PMF analyzes service requirements to automatically determine necessary data sources, preprocessing steps, AI models, and output formats, and creates Pipelines connecting them. Complex services are implemented in collaboration with multiple microservices or existing implementations, automatically orchestrating call sequences, data delivery, error handling, and transactions between microservices. At this time, distributed system patterns are applied to ensure consistency and stability between services, and resilience patterns such as circuit breakers, retries, and timeouts are automatically applied to prevent failures of some services from spreading to the entire system.

3.4.3 AI-powered Autonomous Operation

In the 6G era, network environments where large-scale network data-based services and Edge nodes operate simultaneously are expected. With this increasing complexity, traditional manual operation method fails to consistently ensure operational stability and efficiency, and increasing operational personnel is not sustainable from an RoI (Return on Investment) perspective. DIVE supports AIOps Copilot, an intelligent operations Agent that assists operator decision-making by combining LLM (Large Language Model) and RAG (Retrieval Augmented Generation) technologies to solve this problem.

For effective operation of AIOps Copilot, optimal collection of observability data from the DIVE platform itself should precede. To achieve this, Metrics, Logs, and Traces are collected in an integrated manner from each microservice and node of the DIVE platform based on OpenTelemetry standards [9]. Metrics are stored in time-series databases and utilized for real-time monitoring and anomaly detection, Logs are collected in central log repositories in structured schema-less format to enable search and analysis, and Traces visualize inter-service call relationships and performance bottleneck points through Distributed Tracing systems.

AIOps Copilot provides operators with integrated dashboards and Reference Links to intuitively understand the complex system state of DIVE. Anomaly Detection algorithms detect signs deviating from normal ranges in real-time by combining time-series pattern analysis, statistical outlier detection, and AI-based prediction models. When anomalies are detected, the RCA (Root Cause Analysis) engine operates to track the root causes of failures. RCA identifies service dependency relationships through Topology Graphs and analyzes failure propagation paths along Trace Correlation to determine impact scope and priorities. The intelligent analysis system utilizing LLM and RAG builds a Knowledge Index of past platform failure cases, policy documents, Runbooks, change histories, etc., and periodically updates it. When failures occur, the LLM searches for past cases similar to the current situation and presents related documents and resolution methods through RAG.

AIOps Copilot proposes automatic actions based on predefined Runbooks for detected abnormal situations. For example, when response time for a specific service exceeds thresholds, it presents action scenarios such as 'instance scale-out', 'Circuit Breaker activation', and 'traffic bypass' with priorities. After operator approval (Approval Workflow), actual control commands are delivered to the DIVE Orchestrator through Function Calling mechanisms, and execution results are monitored. All automatic action histories are recorded in Audit Logs for utilization in post-analysis and regulatory response.

Additionally, to support knowledge-based operations, past failure histories, action results, Runbooks, policy change histories, etc., are indexed and stored in Vector Databases (Vector DB). When operators query in natural language, related documents are searched through RAG Pipeline and the LLM generates contextually appropriate answers. Additionally, answer accuracy is improved through continuous feedback learning.

The Self-Healing mechanism prevents failures in the DIVE platform in advance and rapidly recovers failures once occurred. Machine learning-based prediction models learn and detect early signs of service failures such as abnormal memory usage increase patterns, CPU temperature rise trends, and gradual response time increases. When failures are predicted or actually occur, the Self-Healing engine automatically executes recovery procedures, and for minor failures, automatically performs actions such as service restarts and resource reallocation.

3.4.4 Dual Plane Deployment

Network data services in the 6G era should be rapidly developed and deployed in line with the requirements of various industries and customers.

DIVE adopts a Dual Plane Deployment strategy of Governance Plane and Delivery Plane for this purpose. The Governance Plane maintains policy consistency and security control through CSF-centered central governance, while the Delivery Plane is structured to guarantee operational executability of field services through ESF.

More specifically, the Governance Plane manages Declarative policies like the GitOps approach by storing service definitions, network policies, and security rules in code form in Git repositories and tracking change histories. When policy changes occur, they are automatically verified, tested, and approved through CI/CD Pipelines before being deployed to all or some Edge nodes. At this time, differences between Desired State and Actual State can be continuously monitored and automatically adjusted [10].

The Delivery Plane is responsible for rapidly deploying containerized packaged services to the Edge. Using packaging tools, service-specific dependencies, configuration parameters, and resource requirements are declared, and deployment logic is automated. Particularly through Fast Rollout/Rollback capabilities, if performance degradation or errors are detected after deploying new versions, automatic restoration to previous versions is possible within a short time, and stability can be verified through Canary Deployment strategies before gradually expanding.

This Dual Plane Deployment approach enables both consistent policy management centrally and agile service execution at the Edge, and can configure independent Pipelines and serving environments for each service, efficiently satisfying each customer's requirements even in Multi-tenancy environments.

3.4.5 Zero Trust Architecture

DIVE adopts a Zero Trust security model, applying the principle of never trust, always verify all access and transactions. Strong identity authentication is performed at both Edge and Cloud, and communication among microservices within DIVE is encrypted through mutual TLS authentication. Each service can only access necessary resources according to the principle of least privilege, and implements fine-grained permission management by combining role-based access control and attribute-based access control.

An AI-driven security analysis engine detects anomalies by analyzing DIVE's internal traffic patterns, user behavior, and system logs in real-time. Abnormal data access patterns, connection attempts from unknown sources, and abnormal resource usage surges can be signals of security threats. For detected threats, actions such as isolation, blocking, and additional authentication requirements are automatically executed, and real-time notifications are delivered to the security operations center.

Data processing and storage comply with international personal information protection regulations such as GDPR and CCPA, and data access histories are transparently managed through audit logs. Sensitive data at the Edge can be processed only locally without transmission to the cloud by applying Federated Learning methods to enhance privacy. Security in distributed environments faces challenges of maintaining an overall consistent security posture while each Edge and Cloud system independently applies security policies. DIVE manages integrated security policies through the Cloud's Governance Plane and deploys policies to each Edge to guarantee consistency. Simultaneously, Edge nodes can autonomously apply local security policies even when disconnected from the cloud, preventing security gaps.

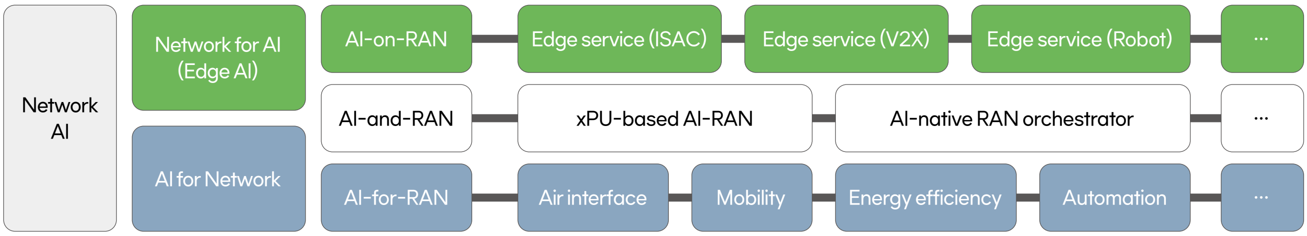
4. SK Telecom's R&D Status and Plans

In this section, we will look at the current status and future plans of R&D, such as PoC (Proof of Concept), that SK Telecom is promoting in each network domain for the mid- to long-term Telco Infra structure innovation/evolution discussed in Section 2.

4.1 AI-native RAN

4.1.1 AI-RAN (AI Integration)

SK Telecom is actively conducting research to improve base station performance by utilizing AI. As a representative example, in September 2022, in a specific test environment, SK Telecom confirmed a transmission speed improvement of approximately 10% by applying AI to Link Adaptation technology. Additionally, since 2023, research has been underway to apply AI to wireless modulation and demodulation technology between base stations and user equipment through collaboration with global operators and manufacturers. Through PoC for this technology, feasibility of transmission speed



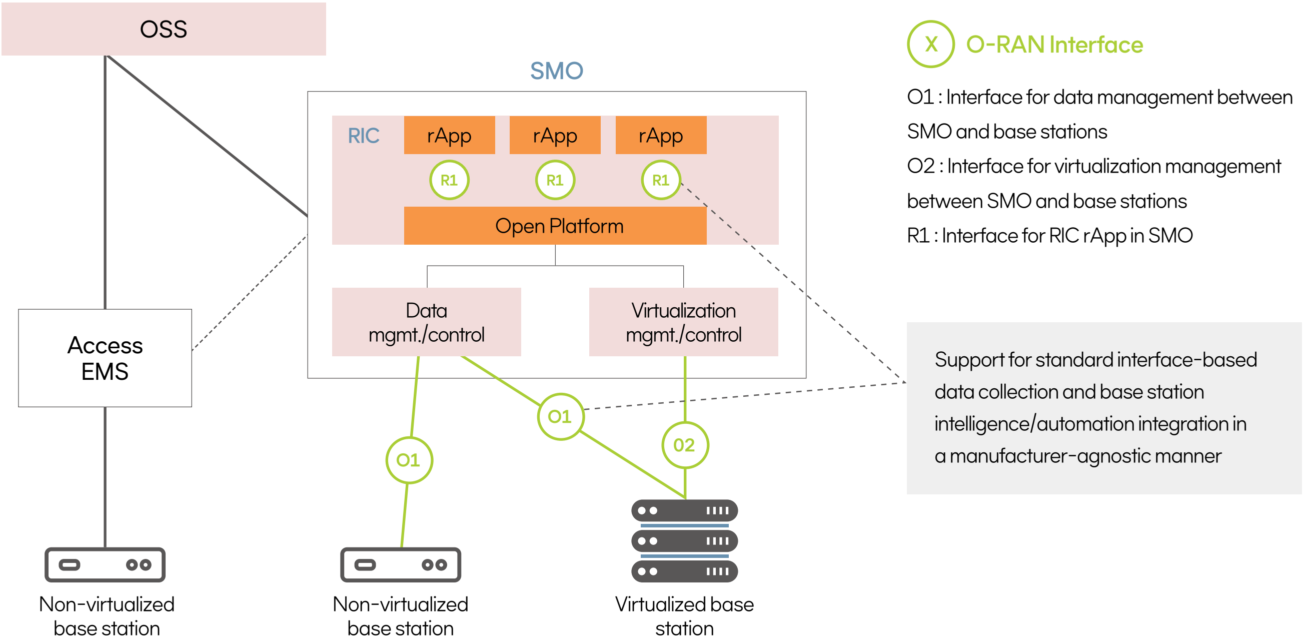
[Figure 10] AI-RAN Domains and R&D Topics improvement has been verified[11], and in recognition of this achievement, SK Telecom won the Future Innovation Award at WCA (World Communication Awards) 2024. Related research continues, including research on AI/ML-based uplink channel estimation and performance improvement in September 2025.

Additionally, research is underway on base station equipment based on various chipsets including GPUs and virtualized resource allocation technology to derive the optimal AI-RAN architecture capable of simultaneously providing communication services and AI services. At MWC 2025, demonstrations were presented showing RAN workload processing utilizing GPUs through L1 Benchmark Test and simultaneous provision of communication services and AI services on a single hardware.

Furthermore, SK Telecom joined the AI-RAN Alliance in October 2024 and is pursuing global activities related to AI-RAN, including proposing and obtaining approval for AI-for-RAN-related items in June 2025, continuing to lead research and development in AI-RAN through collaboration with manufacturers and academia-industry partners.

4.1.2 RAN Automation and Optimization

With the emergence of the O-RAN Alliance, SMO (Service Management and Orchestration), RIC, and related interfaces such as O1, O2, and R1, which were not previously defined in 3GPP, are being standardized [Figure 11].



O1 : Interface for data management between SMO and base stations
O2 : Interface for virtualization management between SMO and base stations
R1 : Interface for RIC rApp in SMO

Support for standard interface-based data collection and base station intelligence/automation integration in a manufacturer-agnostic manner

[Figure 11] O-RAN SMO/RIC Architecture

Simultaneously, various RIC Applications (e.g., rApp) and use cases are being studied and developed. SK Telecom is conducting technical PoCs for various RIC use cases through collaboration with major manufacturers. In 2022, based on collaboration with main equipment vendors, technical PoCs were conducted for congestion control and In-service Software Upgrade, and related achievements were exhibited at MWC 2023. In 2023, PoC was conducted with main equipment vendors for AI-based power saving use cases, and in 2024, PoC was conducted for AI-based power saving use cases with a configuration of heterogeneous manufacturer RIC, rApp, and base station Emulator. These results were also disclosed through O-RAN Alliance PlugFest Fall 2024. Additionally, in September 2024, AI-based base station parameter optimization technology development was completed to improve customer-perceived quality and applied to parts of the commercial networks.

Meanwhile, SK Telecom is also continuously pursuing Orchestrator research to maximize AI-native RAN performance and improve operational efficiency. Through xPU resource allocation technology for simultaneously providing communication and AI services and traffic pattern prediction models trained based on SK Telecom's operational data, research focuses on technologies to increase resource utilization by allocating idle computing resources to AI workloads during low network load periods and to prevent service quality degradation by rapidly converting AI workload resources to RAN workloads during traffic surge situations. Moving forward, SK Telecom plans to secure technological leadership from an AI-RAN Architecture perspective through standardization of key AI-native RAN Orchestrator technologies and ecosystem collaboration PoCs.

Going forward, SK Telecom plans to continue related R&D activities including discovering differentiated RIC use cases such as AI agent solutions for network security enhancement, efficiency improvement through AI integration and commercial environment Trials, and advanced orchestration research.

4.1.3 Base Station Virtualization (RAN Virtualization)

SK Telecom is continuously pursuing research for base station virtualization. In 2019, it became the world's first to commercialize 5G services utilizing virtualized CU, and in 2022, research results on 5G virtualized base stations with equipment manufacturers were presented at MWC 2022. Additionally, through continuous research, performance improvements and advantages and disadvantages according to the diversification and evolution of RAN-dedicated accelerator technology were demonstrated and analyzed. Meanwhile, to improve power consumption of virtualized base stations, AI-based CPU power consumption optimization (C-State Optimization) technology was developed together with major manufacturers. Based on these research achievements in virtualized base stations, in February 2024, a technical white paper on virtualized base stations was jointly published with a major Japanese operator, presenting key considerations and evolution directions for virtualized base stations[12].

Furthermore, SK Telecom is performing development and verification of virtualized base station architectures based on various xPUs including GPUs from a chipset diversification perspective and virtualization-specific functions such as Resource pooling. Based on these research achievements, mid-to long-term R&D on virtualization, a core technology for evolution toward AI-native RAN, will continue to be pursued.

4.1.4 Open Interface

Since pursuing the world's first 5G commercialization in April 2019, SK Telecom has conducted various open interface research and development activities. In the early 5G period when open standard specifications such as those from the O-RAN Alliance were not highly mature, an LSH (Layer Split Hub) in-building solution was developed based on internally defined open fronthaul interface specifications, interworking and commercializing 5G RUs from domestic small and medium-sized enterprises with DUs from main equipment manufacturers.

Subsequently, as standard maturity for open fronthaul interfaces centered on O-RAN Alliance WG4 (Working Group 4) matured, SK Telecom interworked O-DU and O-RU from domestic mid-sized enterprises based on O-RAN Alliance open fronthaul standards in 2022. Additionally, in February 2023, specialized services were interworked and demonstrated in in-building environments, with results presented at MWC 2023.

In 2023, main equipment vendor O-DU and domestic mid-sized manufacturer O-RU were interworked based on O-RAN Alliance open fronthaul standards, and in 2024, success was achieved in interworking main equipment vendor virtualized base stations with domestic mid-sized manufacturer O-RUs.

Additionally, SK Telecom has been conducting R&D activities on the O1 interface, an open interface between SMO and DU, and the R1 interface, an open interface between Non-RT RIC (non-Real Time RIC) and rApp. In 2024, SMO/RIC, rApp, and DU Emulator from heterogeneous manufacturers were interworked, specification conformance for O1 and R1 interfaces was tested and submitted to PlugFest Fall 2024, with achievements recognized.

Furthermore, to secure high-quality, normalized data essential for realizing AI-native RAN based on open interfaces, the Filtered Measurements Feature was proposed in the O-RAN Alliance, and standardization activities are being promoted in WG1, WG10, and others.

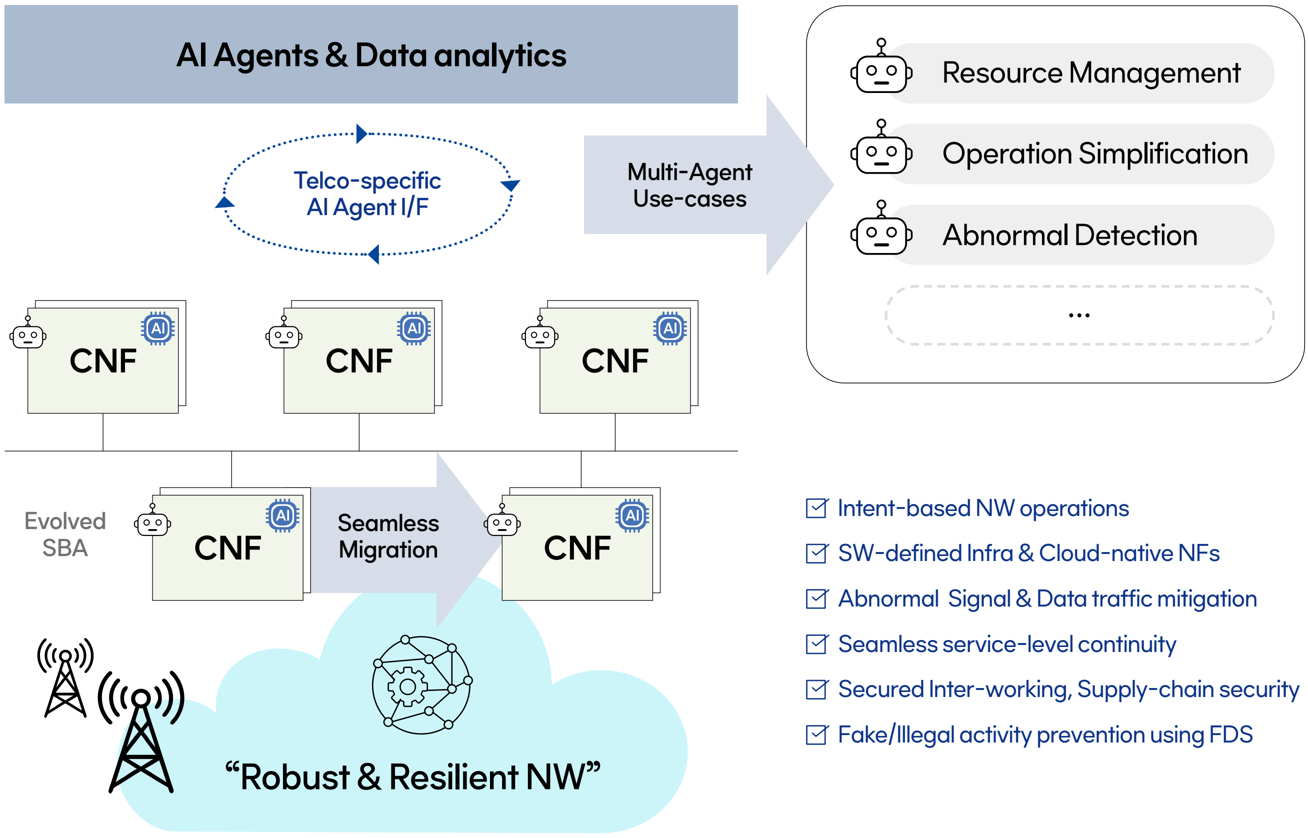
Moving forward, SK Telecom plans to continue building the ecosystem through standardization activities for major interfaces comprising AI-native RAN and demonstration activities such as PoCs and Trials following technology evolution, and plans to conduct research to realize Zero Trust Architecture including continuous mutual authentication and traffic encryption between internal equipment functions and between equipment in line with open interface introduction.

4.2 xCore

4.2.1 AI-native Core

Core network operations have been designed and developed with structures dependent on static rules and manual procedures. When failures or congestion situations occurred, responses were made step-by-step according to predefined rules and operator instructions, functional automation existed sporadically, and linkage between systems was insufficient. Consequently, the level could not escape the premise of operator approval and direct intervention for each case for system-specific operations.

With continuous system advancement and new function introduction, and technology evolution, demands for network simplification from an operational perspective and function alignment are growing to efficiently operate core networks with exponentially increasing complexity. Therefore, evolution toward AI-native Core can accelerate technical evolution of core networks to secure higher levels of quality and service competitiveness while simultaneously pursuing simplified improvement experiences


AI Agents & Data analytics
Telco-specific
AI Agent I/F
Multi-Agent
Use-cases
Resource Management
Operation Simplification
Abnormal Detection
...
AI
CNF
CNF
CNF
Evolved
SBA
CNF
Seamless
Migration
CNF
"Robust & Resilient NW"
☑ Intent-based NW operations
☑ SW-defined Infra & Cloud-native NFs
☑ Abnormal Signal & Data traffic mitigation
☑ Seamless service-level continuity
☑ Secured Inter-working, Supply-chain security
☑ Fake/Illegal activity prevention using FDS

[Figure 12] AI Agents & Data Analytics, Robust & Resilient NW for xCore Architecture from system operation and service TTM perspectives.

To overcome these limitations for evolution toward the future core network outlined earlier, SK Telecom first converted network architecture to standard SBA for gradual autonomation and AI integration. By operating this in a Cloud-native environment, service functions were modularized and development and deployment were made flexible. Subsequently, evolution to Service Mesh architecture efficiently connected various service functions, securing foundation technologies for future core networks[13]. Simultaneously, based on international ETSI NFV and 3GPP standards, standardization activities are being actively conducted by leading technical specifications (Rel-19/Rel-20) for QoS quality assurance utilizing AI and NWDAF and abnormal equipment operation prediction/action[14][15]. Through collaboration with global telecommunications companies and manufacturers, research is actively progressing on network stability and operational efficiency including future 6G AI, xPU, and LLM technology evolution[16][17][18]. Among AI commercialization cases from customer and network quality perspectives, Smart Paging dynamically adjusted Paging areas by reflecting time-of-day and location-based movement patterns, reducing unnecessary signaling load and improving response performance[19]. Additionally, spam filtering introduced functionality to automatically identify fraud risks by learning content and transmission patterns[20].

In the future, core networks plan to evolve into Autonomous Networks—fully autonomous operating platforms that autonomously perform real-time optimization, recovery, and security—for functional expansion toward 'Agentic Core' [Figure 12].

4.2.2 Cloud-native

Core networks have been pursuing full-scale virtualization transformation since 5G commercialization in April 2019. Complex design and verification difficulty has been required to develop single switches that simultaneously process equipment and functions of different generations such as 3G, LTE/NSA, and SA. Additionally, with operation of various generation equipment and interworking through complex call processing protocol interfaces between equipment, E2E analysis and recovery are difficult when unexpected failures or overload/hangups occur. This structural complexity requires equipment/function simplification and failure resilience strengthening, as failure of one element can cause cascading service disruptions.

SK Telecom is continuously pursuing improvements in the virtualization field to overcome these problems, and is jointly proposing various requirements and improvement tasks such as operational efficiency, zero-touch automation, and Observability enhancement with global operators and manufacturers for MANO evolution of ETSI NFV and Telco Cloud transformation[21][22][23]. Based on this, the goal is to secure interoperability, operational simplification, and TCO efficiency through platform services such as

Telco PaaS introduction and linkage with standards and open source.

For evolution toward the future core network forecasted earlier, SK Telecom preemptively developed and commercialized integrated "LTE/NSA+SA switches" (e.g., MME+AMF, S/PGW-C+SMF, S/PGW-U+UPF) at the switch-unit level that integrated equipment of different generations to improve this structural complexity and enhance operational efficiency. Physical equipment numbers decreased and SK Telecom subscriber accommodation capacity was maximized compared to general switches through signaling/data processing efficiency[24][25][26][27].

For effective conversion of PNF (Physical Network Function)/VNF (Virtualized Network Function) to CNF (Cloud-native NF), complex conversion and design of core functions (Control, Data, OAM) to MSA is important. Particularly, operational stability is being verified through Auto-scaling at the Pod unit within CNF, independent deployment, Dynamic Load Balancing through Cluster/Region-wide expansion environments, All-Active call processing, and Error/Fault Isolation, significantly improving network resource efficiency and service launch speed. Additionally, as part of technical review for this, SK Telecom is currently conducting research and commercial development on work to reduce failure occurrence points (e.g., Load Balancing structure algorithms[28], hardware acceleration[29], low-latency critical packet priority processing[30], and NF Parameter optimization). To guarantee uninterrupted voice/data sessions per subscriber, methods to seamlessly and automatically hand over traffic without service quality degradation through NF Set technology and Service Communication Proxy technology[31] even when switch-unit failures occur, and operational methods such as equipment structural improvement and CI/CD to increase verification speed are continuously being improved.

Core networks were designed for server equipment to always operate at maximum performance for service quality and reliability reasons, but core equipment has high idle power consumption even during late night or low load, with room for improvement from carbon emission and energy efficiency perspectives. Therefore, SK Telecom developed Dynamic Power Saving technology without service quality degradation for core equipment to save energy[32][33]. In virtualized environments, power saving effects were confirmed through hardware resource control of core network servers according to real-time traffic conditions dynamically and constantly regardless of times of low or high traffic load, with expansion to all sections and derivation of operational standards underway.

SK Telecom operates a phased conversion roadmap to CNF through PNF or VNF Fadeout (system Rebuilding) with the goal of a complete Cloud-native environment (Cloud-native NF), and is conducting technical review and commercial network application promotion in parallel for container orchestration, service modularization, and distributed deployment policies. Evolution is progressing from the existing 'switch-unit management/operation' system to a Common hardware Pool concept, with plans to simultaneously operate automated verification systems and Staging System with commercial networks for timely commercialization. Additionally, plans are to create automated software installation/control and consistent monitoring by equipment type and service through SDI and NFV orchestration solutions.

4.2.3 Service Enabling Technologies

SK Telecom is expanding B2B/B2G markets by providing APIs and other capabilities to external partners[34], and has completed development of Number Verification API with stronger security than currently used SMS authentication. This signifies transformation toward platform-based networks beyond simple network connectivity.

SK Telecom provides application-specific customized network services based on Network Slice[35] (Slice-based management, security policies, dynamic resource allocation automation) in smart factories, media, public safety, etc., strengthening technological competitiveness through product design satisfying SLA-based service quality in collaboration with customer companies.

SK Telecom is collaborating with global B2B partners for Roaming Edge Cloud[36] evolution, expanding Global Connectivity through this. This architecture provides services that minimize latency and maximize quality by processing data traffic in regions closest to customers roaming abroad.

4.2.4 Zero Trust Architecture

SK Telecom pursues ZTA for security enhancement and is conducting detailed reviews and improvements by purpose for each equipment and service based on GSMA[37][38] and KISA[39] security guides. Through this, various security elements such as communication paths, storage, and authentication procedures are being systematically inspected. Ultimately, technical foundations are being established to lead security frameworks suitable for the 6G era, and security and resilience across all core network sections are being systematically advanced through telco security governance.

Currently, software supply chain security has established itself as an essential requirement for telecommunications network operation, with practical PoCs and commercial applications expanding. SK Telecom has built systems for automatic SBOM (Software Bill of Materials) generation, real-time vulnerability detection, and security patch automation when introducing core equipment and software, applying integrity verification, supply chain risk assessment, and security authentication processes to commercial networks, and operating supply chain risk analysis systems to lead security incident prevention. Supply chain security levels are being improved through strengthening security cooperation with partners, supply chain security education, and real-time monitoring system establishment, contributing to network reliability assurance through PoC and commercial application.

Inter-equipment communication and DB encryption are essential to protect customer data and network information from external attacks or internal leakage, and SK Telecom is securing data flows and enhancing security by encrypting stored log/trace data for this purpose. Particularly as AI-based analysis is applied and more sensitive information is handled, encryption is becoming a fundamental premise of technology development. SK Telecom is researching the latest encryption algorithms and platforms such as PQC, Confidential Computing, and homomorphic encryption to stay ahead in security.

Based on Micro-segmentation[40] within Cloud-native environments, unnecessary access within networks can be blocked and customized policies can be applied by function, simultaneously securing operational efficiency and stability. SK Telecom researched these Observability technologies to implement efficient Deep data collection and analysis systems for communication flows between container Pods utilizing In-NW-Computing[41][42][43], enabling faster and more precise data extraction and monitoring, and demonstrated real-time inter-Pod traffic Anomaly Detection functionality through AI-based analysis. This clarified boundaries between services to enhance security and Visibility, establishing foundations for rapidly detecting abnormal signs.

Recently, financial crimes exploiting mobile telecommunications networks such as identity theft and illegal spam have emerged as social problems, further emphasizing the roles and responsibilities of mobile telecommunications operators. SK Telecom has established and operates FDS (Fraud Detection System) and SFS (Spam Filtering System) capable of detecting and blocking illegal terminals, illegal SIMs, and illegal spam messages within mobile telecommunications networks to protect customers from these threats, learning vast communication patterns and message data through AI technology integration and continuously improving accuracy by advancing AI algorithms. In the future, plans are to evolve these into platforms responding to new crimes such as financial fraud, smishing, and voice phishing by integrating threat information sharing systems with domestic and international security agencies and financial institutions into FDS and SFS.

4.2.5 Centralized DC

SK Telecom is demonstrating core network latency optimization utilizing forward UPF deployment and NWDAF-based analysis. Operational technologies are being developed to preemptively prevent customer-perceived quality degradation by predicting abnormal equipment operation and network congestion in advance through AI, and ultra-low latency service architectures are being implemented by forward-deploying UPF near base stations to process AI services and resources through shortest paths. Additionally, open Network Exposure systems are being built that open network functions to external services through API interworking. Meanwhile, SK Telecom has verified core resource automation and operational advancement technologies utilizing AI Orchestrator and SDI. Based on these R&D achievements, plans are to further strengthen technologies such as AI-based Intent networking to control network resources based solely on operator intent and implement intelligent service openness.

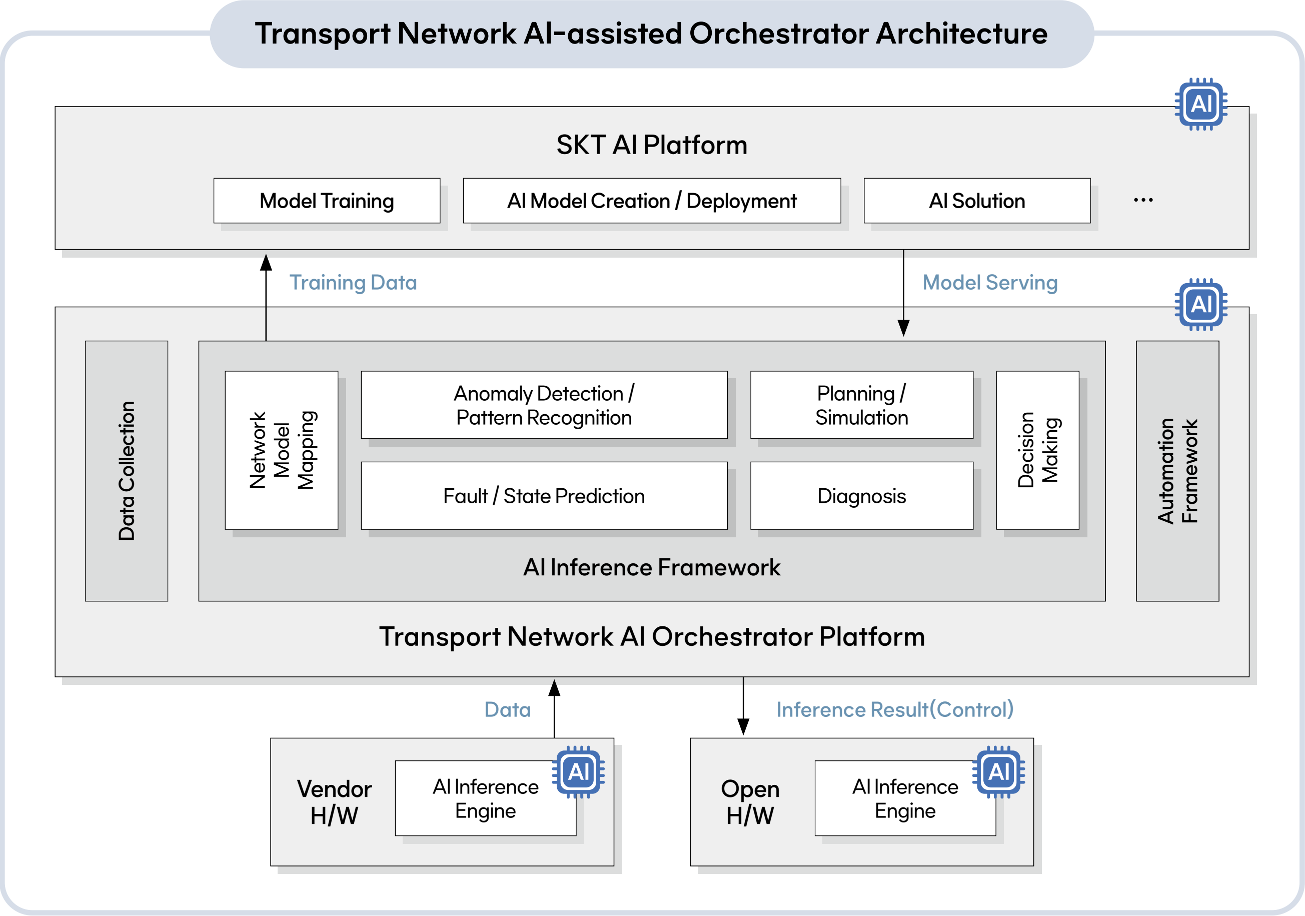
4.3 ACTN

4.3.1 AI-assisted Orchestrator

AI-assisted Orchestrator is being developed as a core technology to realize AI-native Converged Transport Network. It plays a role in innovatively enhancing network efficiency and stability by performing real-time data collection, AI-based analysis, and automated control in an integrated manner across all transport network sections.

AI-assisted orchestrator consists of a data collection module, AI inference framework, and automation framework. The data collection module collects and refines real-time data from equipment of various manufacturers, the AI inference framework is responsible for model management, inference execution, network performance optimization, and decision support, and the automation framework controls networks in real-time based on AI analysis results. This entire process interworks with SK Telecom's AI platform, supporting the full lifecycle from model training through deployment to operation.

AI-assisted Orchestrator collects Telemetry data from equipment of various vendors across all network sections and automates complex operational decision-making such as failure prediction, anomaly detection, traffic optimization, and resource allocation through AI-based inference engines. In practice, by collecting and analyzing routing change data generated from over 10,000 routers in real-time, abnormal signs are detected early, and when AI presents diagnosis and recovery measures, the automation system immediately executes network recovery. Through this, failure detection time can be



[Figure 13] AI-assisted Orchestrator Architecture

shortened to a matter of seconds.

As a core platform for realizing Autonomous Network and AI-assisted Orchestrator, SK Telecom plans to be applied to open hardware and software-based networks to eliminate vendor dependency and maximize scalability and flexibility.

4.3.2 Next Generation Fronthaul Network Technology

When using PAM4 technology to increase optical line speed, optical link budget becomes insufficient, requiring development of optical amplification technology to compensate for this. Recently developed Bismuth doped fiber amplifier was confirmed to show excellent performance for multi-wavelength amplification providing relatively uniform gain across a wide wavelength range in the O-band. Additionally, DCO (Digital Coherent Optics) technology for high-speed optical transmission of 100Gbps and above has been developed targeting relatively long distances of 80km and above, with development of low-cost and low-power optical module products necessary to suit subscriber networks.

Methods using Optical Switch and methods introducing Packet Switch are being discussed as ways to implement Dynamic reconfiguration functionality support for fronthaul networks. Generally, the method using Optical switch has advantages in investment costs as devices are only added on the central office side, while the method introducing Packet Switch can reduce fronthaul bandwidth requirements through traffic aggregation.

4.3.3 Quantum Cryptography

SK Telecom is continuously researching technologies to reduce costs and expand quantum key distribution systems.

WDM QKD technology is a technique that multiplexes and uses existing transmission data channels instead of using Dark fiber previously used for quantum channels in QKD systems, having the effect of reducing construction costs. Through this, SK Telecom plans to expand promote expansion of B2B quantum cryptography dedicated line services.

QKD systems have difficulty transmitting beyond 80km due to transmission distance limitations, and international connectivity was considered particularly challenging. To overcome these transmission distance limitations, wireless QKD using Free Space Optics is being researched. Wireless QKD technology will first develop ground-to-ground communication to confirm technology feasibility, and is expected to enable long-distance transmission and QKD interworking with regions satellites pass through by mounting on satellites and utilizing satellite-to-ground communication.

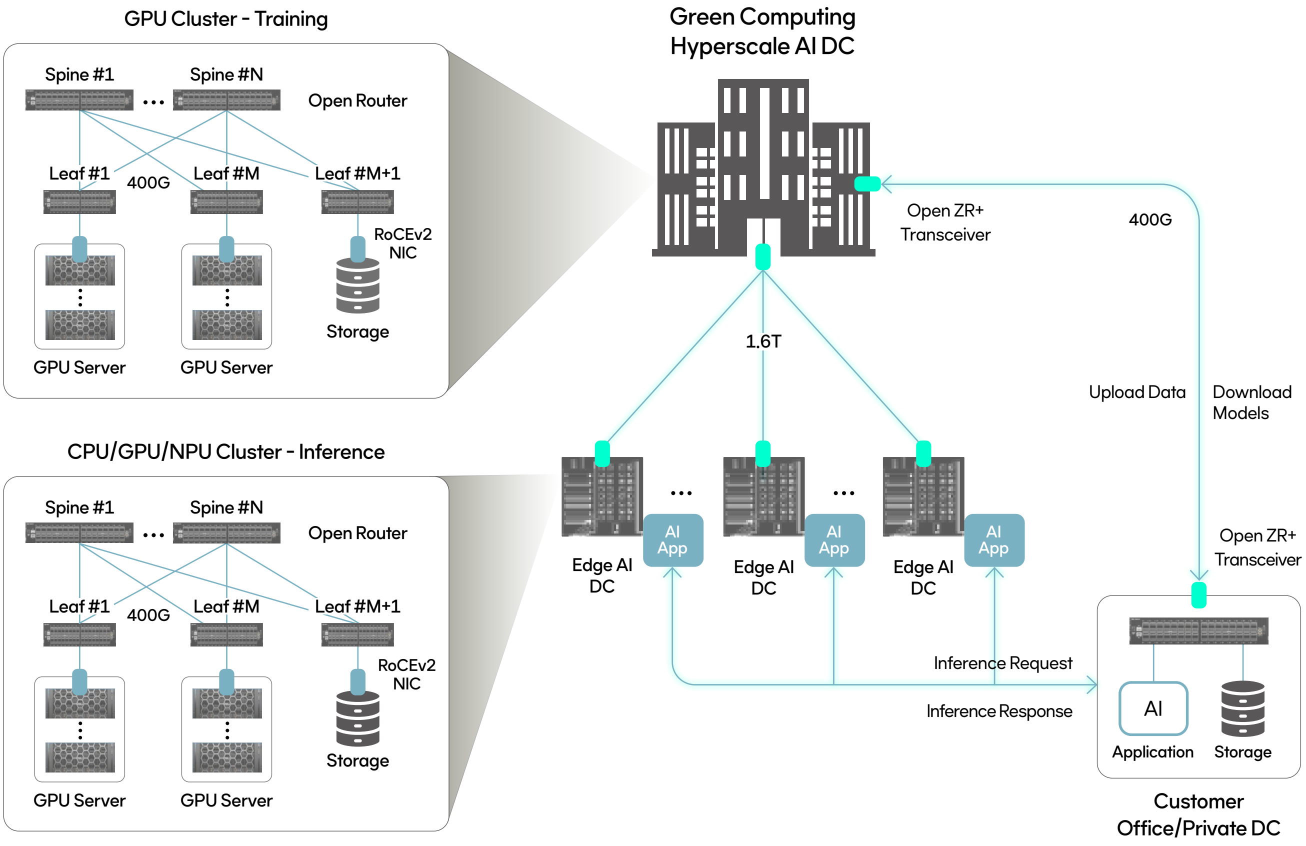
Miniaturized QKD technology aims to develop QKD systems the size of optical modules by integrating QKD systems previously made using optical components through PIC technology.

4.3.4 Cross-DC xPU Clustering Technology

Existing single data center-based GPU clusters have limitations such as throughput variation, resource constraints, and power supply issues. Accordingly, geographically distributed GPU Clustering, where GPU resources distributed across multiple regions are connected by networks to operate like a single integrated computing system—is emerging as a global trend. Major AI service operators are performing large-scale AI model training by connecting multiple data centers, overcoming limitations of power and computing resources.

SK Telecom is building the pilot long-distance inter-central-office GPU Clustering environments by utilizing the latest network equipment such as APN-based Open routers, 400G optical modules, and RDMA (Remote Direct Memory Access) NICs. In test environments, data transmission and AI training performance, latency characteristics, etc., based on RoCE networks are verified. Test environment construction, PoC implementation, performance verification, and result analysis are progressing in stages, with the goal of deriving network architectures suitable for Telco environments based on inter-central-office GPU resource integration and cost-efficient design.

Cross-DC GPU Clustering technology is core infrastructure realizing large-scale distributed training and inference environments for the AI era, strengthening competitiveness through APN-based transport network innovation. In the future, SK Telecom plans to continue advancing technologies in various fields such as efficient orchestration of distributed GPU Clusters, network automation, and service expansion.



[Figure 14] Telco-oriented Cross-DC xPU Cluster

4.4 DIVE

To implement the DIVE platform for the future 6G era, SK Telecom is currently conducting R&D on core DIVE platform design principle technologies, initially limiting network data-based services to precise indoor location-based services targeting B2B customers. Currently, development of Hybrid Edge-Cloud architecture and AI-powered Data Service Development technologies for target services is being pursued, with plans to expand and promote future R&D on DIVE platform-related AI-powered Autonomous Operation, Dual Plane Deployment, and Zero Trust Architecture technologies.

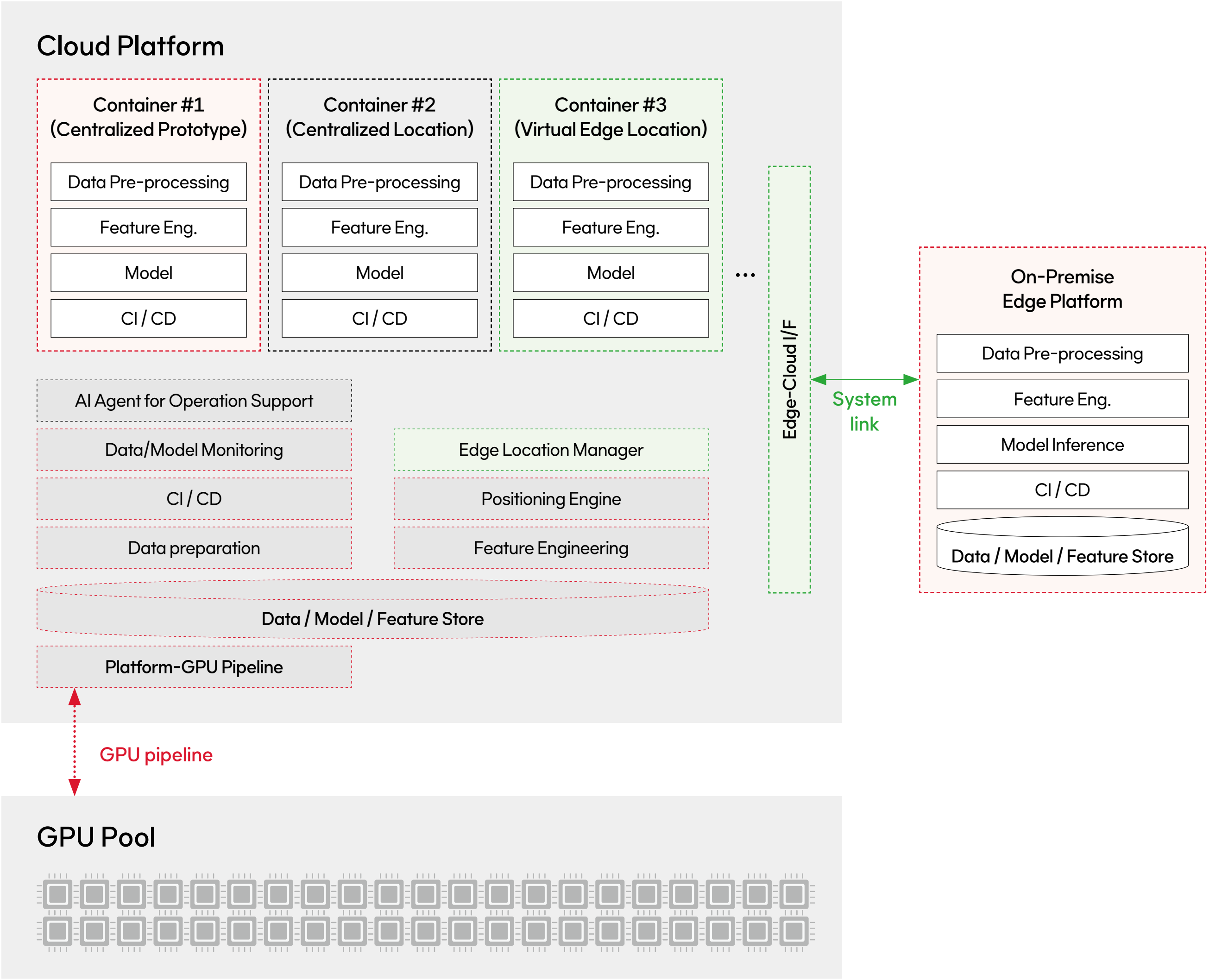
4.4.1 Hybrid Edge-Cloud Architecture

As mentioned earlier, DIVE can overcome limitations in service development and operation of centralized cloud processing methods and Edge-based distributed structures through Hybrid Edge-Cloud architecture.

To achieve this, SK Telecom is conducting R&D on Data-Centric ML/DL Pipeline platforms in the central cloud domain. SK Telecom has established platform architecture design and data preprocessing systems, building scalable data processing architectures utilizing large-scale distributed processing networks for ETL (Extract-Transform-Load) Pipelines for data collection, cleansing, and normalization, and establishing data quality management (Data Quality Check, Schema Validation, etc.) and standard schema-based metadata management systems.

Analysis models are implemented based on Feature Store and Model Registry, establishing foundations for continuous performance improvement through Data-Centric learning strategies. ML/DL-based automated system standardizes data Pipelines through workflow orchestration and distributed learning frameworks, implementing End-to-End automation of model training, validation, deployment, and monitoring by linking with CI/CD and MLOps environments, designed to greatly reduce long-term performance improvement costs.

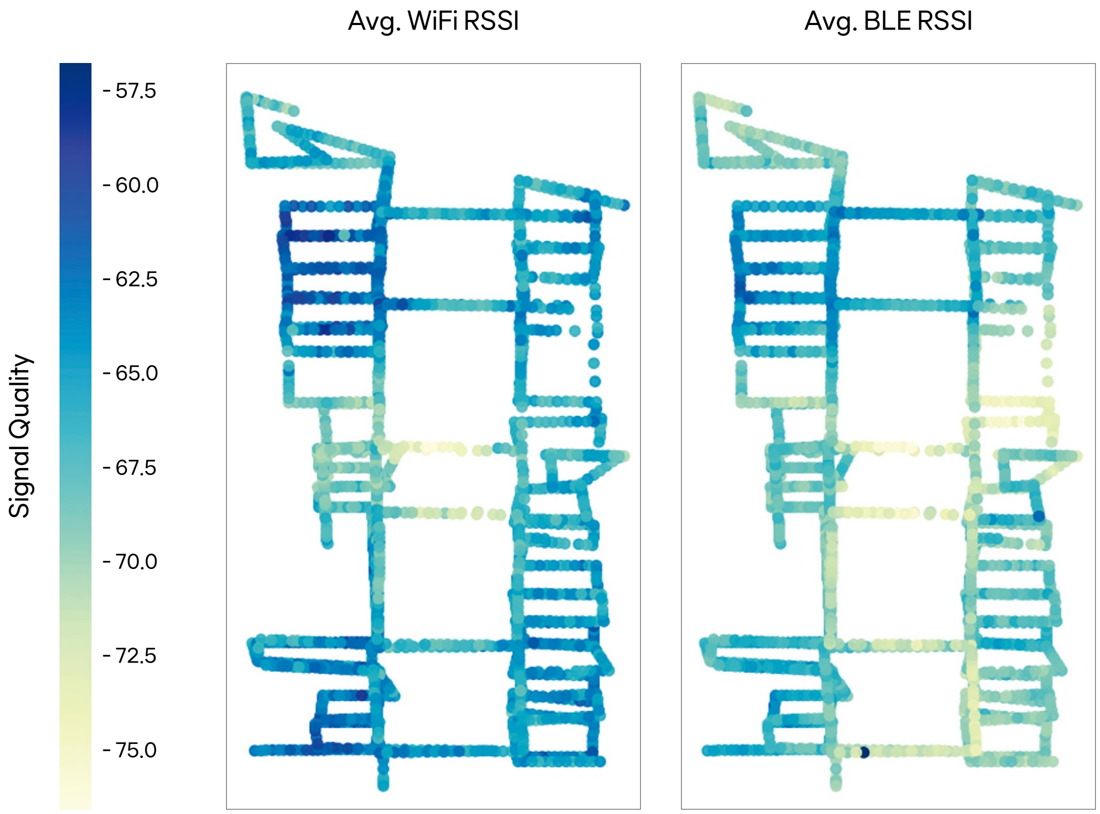
Additionally, in the Edge domain, AI-based Edge Data Service technology development aims to implement field-customized data processing and secure distributed learning environments. To develop and verify precise positioning services based on WiFi and Bluetooth Low Energy in limited indoor spaces, an End-to-End Pipeline including data logging, data cleansing, data analysis, and AI positioning models was configured. Data for this service was collected through Path Planning-based Data Collector Application. Particularly, sensitive data was processed and protected directly at the Edge to minimize security risks in central transmission sections, and continuous model quality improvement was confirmed through data Feedback Loops between Edge and Cloud.



[Figure 15] Hybrid Edge-Cloud Architecture for Location-based Services

Through this, positioning results within 10 meters were achieved, within the test environment at SK Telecom's Pangyo headquarters, and service constraint conditions could be relaxed by applying lightweight AI models to low-specification Edge hardware.

In the future, SK Telecom plans to enhance Hybrid Edge-Cloud architecture completeness, promote scalability verification by applying Federated Learning and Edge-Cloud Orchestration, and develop to enable provision of various forms of data-centric services according to customer requirements.



[Figure 16] Data Collected by Data Collector Application

4.4.2 AI-powered Data Service Development

As mentioned earlier, DIVE is a platform that can transform network data into services. When service planners propose new service ideas, DIVE can rapidly deploy services by automatically configuring necessary network data, models, and Pipelines. While somewhat different in scope and meaning, this is similar to recently emerging AI-based IDE (Integrated Development Environments). Of course, code generated by AI-based IDEs still requires prompt engineering and iterative processes to clearly convey user requirements, and final outputs still fall short of fully satisfying user requirements. However, in the future 6G era, most of these code-level limitations are expected to be overcome, and network data-based services are also expected to enable easier development and deployment according to service planners' requirements in this form.

SK Telecom utilized AI-based IDE to improve developer productivity during the precise positioning service development process mentioned earlier. Through this, Data Collector Application for data collection was developed, and debugging and refactoring work was performed on AI positioning models including Random Forest Regressor, XGBoost, and Transformer. Additionally, lightweight models were rapidly developed by reflecting not only simple requirements but also developer insights to further improve WiFi positioning performance. Through this, feasibility for rapid service configuration and deployment through AI utilization was confirmed in the process of developing network data service components.

5. Conclusion

Since 5G commercialization, the mobile telecommunications industry has changed at an unprecedented pace, and these changes are expected to accelerate further in the 2030s when 6G is fully commercialized. In particular, the convergence of AI and networks, network-computing integration, and the proliferation of data-based new services are expected to fundamentally transform telecommunications infrastructure architecture and operation methods. Simultaneously, the advancement of cyber threats and increasing demands for personal information protection are making security capability enhancement an essential imperative.

Against this backdrop of environmental change, SK Telecom has established six evolution directions—AI-native network, cloud-native network, ubiquitous network, open network, zero trust network, and customer-centric network—and is continuously advancing technologies with goals of maximizing operational efficiency, innovating customer experience, and network-based monetization.

Through this white paper, specific architectures and implementation technologies have been presented centered on AI-native RAN, xCore, ACTN, and DIVE—core areas of mid- to long-term future network evolution. Radio access networks are pursuing AI automation and optimization based on open interfaces and virtualization. Core networks are strengthening autonomous operation and service openness through Cloud-native transformation and AI agent introduction. Transport networks are realizing intelligence and automation by combining digital twin, APN-based architecture, quantum cryptographic communication, and xPU clustering. The DIVE platform aims for self-healing and enhanced security utilizing network data. These visions are linked with current R&D activities, actively promoting AI-based performance improvement and AI service provision at the edge, cloud-native core and security technology advancement, intelligent transport network control and quantum cryptography demonstration, and data platform model quality improvement and edge AI inference support, leading the 6G era through cooperation with the global ecosystem.

The landscape and requirements of the 6G era still involve many uncertainties and variables. Unexpected technology trend changes, global standardization pace, market and policy environment shifts, and new customer needs will require continuous adjustment and refinement. Accordingly, rather than insisting on predetermined answers, SK Telecom prioritizes customer value and will proactively build telecommunications infrastructure for the 6G era through an open and agile approach that can flexibly respond to changes based on Cloud-native, AI-based automation, open interfaces, and zero trust architecture-based security technologies, creating new opportunities in future markets.

References

[1] SK Telecom, "5G Lessons Learned, 6G Key Requirements, 6G Network Evolution, and 6G Spectrum," SK Telecom 6G White Paper, Aug. 2023, https://bit.ly/4a27B9I

[2] SK Telecom, "View on Future AI Telco Infrastructure," SK Telecom 6G White Paper, Oct. 2024, https://bit.ly/4eYS0t1

[3] Samsung Electronics, "AI-Native & Sustainable Communication", Feb. 2025

[4] Ericsson, "Co-creating a cyber-physical world", July 2024.

[5] Nokia, "Nokia's Vision for 2030: Pioneering the Future of Networks", Mar. 2024

[6] ICT R&D Technology Roadmap 2025, p96, IITP (Institute of Information & communications Technology Planning & evaluation), 2024

[7] Gartner, "Hype Cycle for Edge Computing", 2024

[8] CNCF, "GitOps Principles v1.0.0", Cloud Native Computing Foundation, 2023

[9] OpenTelemetry, "OpenTelemetry Specification", 2024

[10] Argo Project, "Argo CD - Declarative GitOps CD for Kubernetes", 2024

[11] K. Lee, et al, "AI-based Pilotless Communication: Experimental Validation via Channel Emulation and Indoor Over-the-air Testing", in the 16th International Conference on ICT Convergence (ICTC) Workshop, Oct. 2025

[12] SK Telecom and NTT DOCOMO, "Key Considerations for vRAN: Insights from SK Telecom and NTT DOCOMO", Feb. 2024

[13] "Toward 6G Core Architecture Using an Inline Service Mesh", SK Telecom & Intel Whitepaper, Jan. 2024

[14] "SK Telecom, S1-242019, 6G Area of Interest", 3GPP SA1#107, Aug. 2024

[15] "SK Telecom, S2-2502989, Views on 6G study in SA WG2", 3GPP SA2#168, Apr. 2025

[16] "AI-agent Communication Network (ACN)" CMCC/MWC White Paper, Mar. 2025

[17] "Leveraging LLM for Evolving and Declarative Trace Analytics towards Next Generation Mobile Core Networks", IEEE FNWF, Oct. 2024

[18] "Dynamic Traffic Load Rebalancing for Hardware-accelerated 6G UPF Resilient Architecture", IEEE IPCCC, Nov. 2024

[19] "SK Telecom upgrades core network with AI technology jointly developed by Samsung Electronics", https://www.etnews.com/20220701000222, Jul. 2022

[20] "SK Telecom Wins 'CES 2025' Best Innovation Award with AI Spam Detection Technology", https://www.etnews.com/20241117000008, Nov. 2024

[21] "In the Light of Ten Years from the NFV Introductory", ETSI Whitepaper No. 53, Feb. 2023

[22] "NFV evolution: Towards the Telco Cloud", ETSI White Paper No. 65, Mar. 2025

[23] "Management and Orchestration of the Telco Cloud: The Role of NFV-MANO and Its Added Value", ETSI White Paper No. 67, May. 2025

[24] "SK Telecom Succeeds in Pure 5G Communication in Commercial Networks", https://news.sktelecom.com/137028, Jan. 2020

[25] "SKT-Samsung Electronics Preempts International Standard Technology for 'Next-Generation Cloud Core Network'", https://news.sktelecom.com/136426, Nov. 2020

[26] "SKT to commercialize 'next-generation 5G Core' next year", https://news.sktelecom.com/172464, Nov. 2021

[27] "SKT Secures Foundation for 6G Evolution by Upgrading Core Network", https://news.sktelecom.com/179973, Jul. 2022

[28] "Implementation for a Resilient Cloud-native Core Network with an eBPF-based SCTP", IEEE FNWF, Oct. 2024

[29] "Towards Achieving High Performance in 5G Mobile Packet Core's User Plane Function", SK Telecom & Intel Whitepaper, Feb. 2018

[30] "Low Latency 5G UPF Using Priority Based 5G Packet Classification", SK Telecom & Intel Whitepaper, Jun. 2020

[31] "Evaluation of a Service-mesh based Service Communication proxy for Future 5G Core Network", SK Telecom & Nokia Whitepaper, Apr. 2020

[32] "Dynamic Power Savings in Cloud-Native 5G", SK Telecom & Intel Whitepaper, Mar. 2023

[33] "SKT Successfully Develops Green Infra Technology with Intel", https://news.sktelecom.com/185221, Feb. 2023

[34] "Three Telecom Companies Strengthen Innovative Service Ecosystem with Common API Standards", https://news.sktelecom.com/206655, Aug. 2024

[35] "SKT Develops App/Service-Specific Network Slicing Technology", https://news.sktelecom.com/136300, Dec. 2020

[36] "Roaming Optimization using Global Presence of AWS: SK Telecom Roaming Edge Cloud", https://aws.amazon.com/ko/blogs/industries/roaming-optimization-using-global-presence-of-aws/, Jun. 2024

[37] "GSMA FS.31 - Baseline Security Controls", https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/fs-31-gsma-baseline-security-controls/, Apr. 2025

[38] "GSMA FS.40 - 5G Security Guide", https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/5g-security-guide-version-3-0/, Jul. 2024

[39] "Zero Trust Guidelines 2.0", https://www.kisa.or.kr/2060204/form?postSeq=18#fnPostAttachDownload, Dec. 2024

[40] "GSMA FS.61 - Micro-Segmentation in 5G Core Network Resource Pool", https://www.gsma.com/solutions-and-impact/technologies/security/gsma_resources/micro-segmentation-in-5g-core-network-resource-pool-guidelines-version-1-0/, Apr. 2025

[41] "Congestion-Aware Selective In-band Network Telemetry for Low Traffic Overhead and High-Accuracy Network Monitoring", IEEE INFOCOM, May. 2025

[42] "Semantic In-Band Network Telemetry for Low Bandwidth Overhead and High-Accuracy Monitoring", IEEE INFOCOM, May. 2025

[43] "FAT-INT: Frequency-Aware and Item-Wise In-band Network Telemetry for Low-Overhead and Accurate Measurement", ACM on Networking, Sep. 2025

Abbreviations

Abbr	Full Name	Abbr	Full Name
APN	All Photonic Network	OT	Operational Technology
CCO	Coverage and Capacity Optimization	PAM4	Pulse Amplitude Modulation 4-level
CCPA	California Consumer Privacy Act	PMF	Pipeline Management Function
CI/CD	Continuous Integration/Continuous Delivery, Deployment	PNF	Physical Network Function
CNF	Core Network Function	PoC	Proof of Concept
CNF	Cloud-native Network Function	POTN	Packet Optical Transport Network
COTS	Commercial Off-The-Shelf	PQC	Post-Quantum Cryptography
CT	Communication Technology	QKD	Quantum Key Distribution
DAF	Data Analytics Function	QKMS	Quantum Key Management System
DCI	Data Center Interconnect	QNF	Quantum Network Function
DCO	Digital Coherent Optics	RAG	Retrieval-Augmented Generation
DIVE	Data Insight & Value Engine	RCA	Root Cause Analysis
Edge UPF	Edge User Plane Function	RIC	RAN Intelligent Controller
EMS	Element Management System	RNF	Radio Network Function
ETSI	European Telecommunications Standards Institute	SA	Standalone
FBS	False Base Station	SBA	Service Based Architecture
FDS	Fraud Detection System	SBOM	Software Bill of Materials
FPGA	Field-Programmable Gate Array	SDI	Software Defined Infrastructure
GDPR	General Data Protection Regulation	SDN	Software Defined Networking
gPRC	Google Remote Procedure Call	SFS	Spam Filtering System
GSMA	Global System for Mobile Communications Association	SLO	Service Level Objective
IOWN	Innovative Optical and Wireless Network	SMO	Service Management and Orchestration
IPoDWDM	IP over Dense Wavelength Division Multiplexing	SPIFFE	Secure Production Identity Framework for Everyone
IT	Information Technology	SPIRE	SPIFFE Runtime Environment
LLM	Large Language Model	SUCI	Subscription Concealed Identifier
MPLS	Multiprotocol Label Switching	TCO	Total Cost of Ownership
mTLS	Mutual Transport Layer Security	TLS	Transport Layer Security
NEF	Network Exposure Function	TNF	Transport Network Function
NETCONF	Network Configuration Protocol	TPU	Tensor Processing Unit
NF	Network Function	VM	Virtual Machine
NFV	Network Functions Virtualization	VNF	Virtual Network Function
NG-ROADM	Next-Generation Reconfigurable Optical Add-Drop Multiplexer	VNF	Virtualized Network Function
NIC	Network Interface Card	WCA	World Communication Awards
Non-RT RIC	non-Real Time RIC	WDM	Wavelength Division Multiplexing
NSA	non-standalone	WG	Working Group
NWDAF	Network Data Analytics Function	ZTA	Zero Trust Architecture
OAM	Operations, Administration, and Maintenance		